

jc525 U.S. PTO
09/277417
03/26/99

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

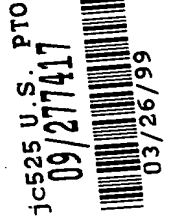
Date of Application: March 26, 1998
Application Number : P10-79837
Applicant(s) : Nippon Telegraph & Telephone Corporation

February 5, 1999

Commissioner,
Patent Office Takeshi ISAYAMA

Number of Certificate: H-11-3003894

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1998年 3月26日

出願番号
Application Number:

平成10年特許願第079837号

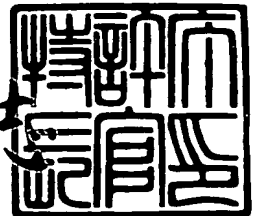
出願人
Applicant(s):

日本電信電話株式会社

1999年 2月 5日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3003894

【書類名】 特許願

【整理番号】 NTTH097177

【提出日】 平成10年 3月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/28

【発明の名称】 接続制御方法および通信網

【請求項の数】 4

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

 【氏名】 久田 裕介

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

 【氏名】 小野 諭

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

 【氏名】 市川 晴久

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

 【代表者】 宮津 純一郎

【代理人】

 【識別番号】 100083806

 【弁理士】

 【氏名又は名称】 三好 秀和

 【電話番号】 03-3504-3075

【選任した代理人】

【識別番号】 100068342

【弁理士】

【氏名又は名称】 三好 保男

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701396

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 接続制御方法および通信網

【特許請求の範囲】

【請求項 1】 通信網において着信者の前記通信網における識別子を隠蔽しつつ、前記通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法であって、

通信網内の第 1 の機関がユーザに役割識別子を付与し、

第 2 の機関が役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能なように保持し、

発信者は前記役割識別子とユーザに関する情報とを対にした情報に基づいて着信者を役割識別子で指定し、

第 3 の機関は前記指定に基づいて前記発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、

第 4 の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、第 4 の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うこと

を特徴とする接続制御方法。

【請求項 2】 前記個別化アクセスチケットに関する第 4 の機関の認証結果が正しくても、着信者が第 4 の機関の着信拒否リストにそのチケットを登録している場合は、第 4 の機関は当該接続要求を拒否することを特徴とする請求項 1 記載の接続制御方法。

【請求項 3】 ユーザの通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの接続を制御可能とする通信網であって、

通信網内のユーザに役割識別子を付与する第 1 の機関と、

前記付与された役割識別子と該役割識別子に対応するユーザに関する情報とを対にして他のユーザから閲覧可能なように保持する第2の機関と、

通信網内の発信ユーザにより、他のユーザがその役割識別子によって着信先として指定された場合に、該役割識別子に基づいて前記発信ユーザに対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行する第3の機関と、

発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、通信網における物理的な接続制御方式に変換することで接続制御を行う第4の機関と

を有することを特徴とする通信網。

【請求項4】 前記第4の機関は、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項3記載の通信網。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法および通信網に関する。

【0002】

【従来の技術】

近年、電話やコンピュータネットワークを用いた個人攻撃、例えば嫌がらせ、名誉毀損等が深刻な社会問題になっている。このような個人攻撃は通信網を介して氏名、性別、年齢、電話番号、電子メールアドレスといったプライバシー情報が第三者に漏洩するために発生するものである。具体的には、第三者による盗聴

、偽装等の盗難、第三者による意図的な収集（アンケート）、発信者の間違い電話等の端末操作ミス、発信者によるやむを得ない公開（情報誌、電子掲示板、ホームページ等）がある。

【0003】

現在、盗難対策には認証、暗号化があり、間違い電話対策には端末の電話帳機能がある。また、第三者によるアンケート等の意図的な収集および発信者によるやむを得ない公開に対しては、いくつかの対策が実施されているが、いずれも漏洩を完全に防止することはできない。

【0004】

求人（仲間募集）や売買のように他のユーザと個人的に連絡を取る必要があるユーザは、最低限、氏名と連絡先を情報誌、電子掲示板、またはホームページに掲載しなければならない。また、性別、年齢といったプライバシー情報を公開しなければならない場合もある。ところが、これらのメディアを閲覧するのは善意のユーザだけではない。個人攻撃を仕掛けようと企むユーザも閲覧する可能性は決して小さくない。そこで、情報を公開したユーザを何らかの手段で個人攻撃から保護することが必要になる。

【0005】

このとき、そのユーザの取り得る戦略は2種類ある。ひとつは情報を限定公開する戦略で、具体的にはニックネームがある。もうひとつは接続相手を着信側で限定する戦略で、具体的には二重番号登録、発信者番号通知、着信拒否、匿名電子メール(Anonymous Mails)がある。

【0006】

インターネットやパソコン通信の電子掲示板システムではニックネーム（ハンドルネーム）による発信が可能のため、実名を隠蔽することができる。しかしながら、善意のユーザにはすべてのプライバシー情報を公開するけれども、悪意のユーザには公開しないといったような制御はできないし、発信者の電子メールアドレスも隠蔽できない。このため、第三者から攻撃される恐れがある。

【0007】

二重番号では、図27に示すように、回線に複数の電話番号を割り当て、その

うちの一部の番号への呼をすべて自動的に切断するため、個人攻撃を被る恐れはない。その代わり、着呼可能な番号を知る者には厳重に守秘義務が課される。

【0008】

また、発信者番号通知は、図28に示すように、発信者電話番号を着信側端末に通知するものであり、アナログ公衆網、ISDN、デジタル携帯網で提供されているが、番号非通知の場合には、着信端末にも何も表示されない。

【0009】

一方、着信拒否は、図29に示すように、呼を自動的に切断する機能であり、アナログ公衆網、ISDN、デジタル携帯網で提供されている。仕様は網によって異なる。アナログ公衆網とISDNでは、着信側回線あるいは端末で指定した発信者番号の呼以外は接続しない。逆に、デジタル携帯網では、着信側端末で設定した発信者番号の呼を切断する。

【0010】

一般に、発信者番号通知と着信拒否は組み合わせて利用される。ところが、両者を組み合わせると、発信者と着信者のいずれか一方しか保護できなくなる。アナログ公衆網やISDNでは番号非通知の呼を切断するため、番号漏洩を防止できなくなる。仕様を逆手にとると、個人情報の収集手段として利用できるからである。一方、デジタル携帯網では番号非通知の呼を切断しないため、着信者を個人攻撃から保護できなくなる。

【0011】

匿名電子メールでは、図30に示すように、発信者メールアドレスをリメーラ(remailer)機能を持つメールサーバのメールアドレスに書き換えて送信先に転送する。このように、発信者メールアドレスを隠蔽するため、発信者メールアドレスの漏洩を防ぐことができる。その一方で、匿名による攻撃が可能になるため、着信者が第三者から攻撃される危険性はより高くなる。

【0012】

これを防ぐために、着信者から要求があった場合には、リメーラはその着信者宛の匿名メールの配信を中止する。ところが、この機能を用いると番号漏洩を防ぐことはできなくなる。着信拒否同様、個人情報の収集手段として利用できるか

らである。

【0013】

【発明が解決しようとする課題】

上述したように、従来のニックネーム、二重番号登録、発信者番号通知、着信拒否、匿名電子メール等の方法では、それぞれ発信者の電子メールアドレスを隠蔽できず、第三者から攻撃されたり、着呼可能番号を知る者に厳重な守秘義務が課せられたり、番号非通知の呼を切断しない場合もあり、着信者を個人攻撃から保護できなかつたり、匿名による攻撃が可能となり、着信者が第三者から攻撃される危険性が高くなるというような種々の問題がある。

【0014】

本発明は、上記に鑑みてなされたもので、その目的とするところは、第三者による意図的な収集およびユーザによるやむを得ない公開に対して匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とし、着信者が匿名性を悪用した発信者による攻撃にさらされた場合には、その攻撃による着信者への被害を食い止めることを可能とする接続制御方法および通信網を提供することにある。

【0015】

【課題を解決するための手段】

上記目的を達成するため、請求項1の本発明は、通信網において着信者の前記通信網における識別子を隠蔽しつつ、他のユーザからの前記通信網における識別子を隠蔽した通信の接続を制御する接続制御方法であって、通信網内の第1の機関がユーザに役割識別子を付与し、第2の機関が役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能なように保持し、発信者は前記役割識別子とユーザに関する情報とを対にした情報に基づいて着信者を役割識別子で指定し、第3の機関は前記指定に基づいて前記発信者に対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、第4の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄され

ていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【0016】

請求項1記載の本発明にあっては、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および、有効期限を含む個別化アクセスチケットを発行し、役割識別子および個別化アクセスチケットを用いて、個別化アクセスチケットに改竄がなく、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという3要件をすべて検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【0017】

また、請求項2記載の本発明は、請求項1記載の発明において、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストにそのチケットを登録している場合は、第4の機関は当該接続要求を拒否することを要旨とする。

【0018】

請求項2記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【0019】

更に、請求項3記載の本発明は、ユーザの通信網における識別子を隠蔽しつつ、他のユーザからの接続を制御可能とする通信網であって、通信網内のユーザに役割識別子を付与する第1の機関と、前記付与された役割識別子と該役割識別子に対応するユーザに関する情報とを対にして他のユーザから閲覧可能なように保

持する第2の機関と、通信網内の発信ユーザより、他のユーザがその役割識別子によって着信先として指定された場合に、該役割識別子に基づいて前記発信ユーザに対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行する第3の機関と、発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、該個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、通信網における物理的な接続制御方式に変換することで接続制御を行う第4の機関とを有することを要旨とする。

【0020】

請求項3記載の本発明にあっては、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、役割識別子、個別化アクセスチケットおよび個別化アクセスチケットに対する電子署名を用いて、個別化アクセスチケットが改竄されていなくて、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという3要件をすべて検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【0021】

請求項4記載の本発明は、請求項3記載の発明において、前記第4の機関が、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【0022】

請求項4記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【0023】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。本発明の接続制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者からの通信をも適宜可能とするものであり、基本的には着信者の本当の識別子を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【0024】

具体的には、図1(a)に示すように、ユーザに対して個人情報隠蔽した役割識別子(Anonymous Identification: AIDと略称する)を付与し、この役割識別子AIDをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【0025】

また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を探すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットPAT(Personalized Access Ticket)を取得する。

【0026】

個別化アクセスチケットPATには、発信者、着信者それぞれの役割識別子AIDの他に、発信者フラグ、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、図1(b), (c)に示すように着信拒否等の接続制御を行うために使用される。すなわち、移転制御フラグを立てると、後述

するセキュア・コミュニケーション・サービス SCS (Secure Communication Service) は、接続要求の際に、発信者に対し、例えば署名の検証、パスワード要求等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービス SCS は認証無しで接続要求をセキュア・コミュニケーション・サービス SCS が接続している物理的通信網に渡す。すなわち、移転制御は役割識別子 AID がこれを認証局 CA (Certification Authority) から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【0027】

本発明の接続制御方法を実施する通信網においては、ユーザに対する役割識別子 AID の付与、役割識別子 AID と組み合わせられた情報の保持、個別化アクセスチケット PAT の発行、および個別化アクセスチケット PAT に基づく接続制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。

【0028】

図 2 は、本発明の一実施形態の全体構成図である。本実施形態はインターネット電子メールシステムを対象としたものである。図 2 において、1 は認証局 CA であり、認証権限と役割識別子 AID の発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。3 はユーザであり、5 はセキュア・コミュニケーション・サービス SCS であり、ユーザ 3 間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。7 はアノニマス・ディレクトリ・サービス ADS であり、役割識別子 AID、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービス ADS 7 は、検索者の役割識別子 AID と検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子 AID から個別化アクセスチケット PAT を発行し、検索者に交付する機能を有する。

【0029】

まず、ユーザの要求に基づいて個人識別子から役割識別子 AID を生成し、そ

のユーザに割り当てるまでの一連の処理について説明する。

【0030】

図3は、個人識別子O I D (Official Identification) と役割識別子A I D の例を示している。同図に示すように、個人識別子O I D は、図3 (a) に示すように認証局C A 1 がユーザに一意に生成した任意の文字列に対して認証局C A 1 が秘密鍵で電子署名したものである。また、役割識別子A I D は、図3 (b) に示すように個人識別子O I D の一部とその位置情報、冗長な文字列、S C S のホストO I D からなる文字列に対し、認証局C A 1 の秘密鍵で電子署名を施したものである。

【0031】

次に、ユーザ3が役割識別子A I D を認証局C A 1 に対して請求する処理について図4に示すフローチャートを参照して説明する。ユーザは個人識別子O I D と請求項目を入力して(ステップS 4 1 1)、図7に示すようにA I D 請求メッセージを作成し(ステップS 4 1 3)、ユーザO I D の秘密鍵で署名、暗号化し(ステップS 4 1 5)、それから該A I D 請求メッセージを認証局C A 1 に電子メールで送信する(ステップS 1 4 7)。

【0032】

A I D 請求メッセージは、発信者の個人識別子O I D と請求項目から構成され、請求項目は次に示す2種類のうちのいずれかである。

(1) 新規な役割識別子A I D の割り当てを要求する場合：

REQUEST AID <要求するA I D の数>

(2) 既存の役割識別子A I D の廃止を要求する場合：

DISCARD AID <廃止したいA I D の実体>

【0033】

次に、上述した役割識別子A I D の請求に対する認証局C A 1 が役割識別子A I D をユーザ3に対して交付する処理について図5に示すフローチャートを参照して説明する。図5において、認証局C A 1 は、ユーザ3からの上述したA I D 請求メッセージを受信すると(ステップS 5 1 1)、認証局C A 1 はユーザ3のO I D 公開鍵を用いてA I D 請求メッセージ(図7)を復号化、認証する(ステ

ップ S 5 1 3)。認証局 C A 1 は該メッセージが改竄されているか否かをチェックする（ステップ S 5 1 5）。改竄を検出した場合には、該メッセージを破棄するが、改竄が認められなかった場合には、認証局 C A 1 は役割識別子 A I D を生成し（ステップ S 5 1 7）、A I D 秘密鍵および A I D 公開鍵を生成し（ステップ S 5 1 9）、図 8 に示す A I D 交付メッセージを生成する（ステップ S 5 2 1）。それから、認証局 C A 1 は該メッセージをユーザ O I D の公開鍵で署名、暗号化し（ステップ S 5 2 3）、この署名したメッセージをユーザ 3 の O I D に送信する（ステップ S 5 2 5）。

【0034】

次に、図 6 に示すフローチャートを参照して、ユーザにおける A I D 交付処理について説明する。図 6 において、ユーザ 3 が認証局 C A 1 からの暗号化された A I D 交付メッセージを受信すると（ステップ S 6 1 1）、ユーザ 3 はユーザ秘密鍵を用いて A I D 交付メッセージを復号化、認証し（ステップ S 6 1 3）、該メッセージが改竄されているか否かをチェックする（ステップ S 6 1 5）。改竄を検出した場合には、エラーメッセージを出力し、該 A I D 交付メッセージを破棄する（ステップ S 6 1 7）。また、改竄が認められない場合には、A I D 交付メッセージから役割識別子 A I D と A I D 秘密鍵を抽出し、ユーザ 3 に通知する（ステップ S 6 1 9）。

【0035】

A I D 交付メッセージは、図 8 に示すように発信者 O I D と処理結果から構成されている。処理結果は次に示す 2 種類のうちのいずれかである。

(1) 新規な役割識別子 A I D の交付の場合：

NEW AID <新規 A I D の実体と A I D の秘密鍵 | A I D 取得失敗>

(2) 既存の役割識別子 A I D の廃止

DISCARD AID <既存 A I D の実体><廃止完了 | 廃止失敗>

【0036】

次に、認証局 C A における役割識別子 A I D の生成処理について図 9、図 10 を参照して説明する。図 9 において、認証局 C A 1 は乱数発生等の任意の手段を用いて、個人識別子 O I D の全長 L と等しい長さの文字列を生成し、この文字列

を仮の役割識別子 A I D として生成する（ステップ S 9 1 1）。

【0037】

次に、個人識別子 O I D の複写を行うために、個人識別子 O I D のコピー範囲を指定する p と l の値を決定する（ステップ S 9 1 3）。これは、乱数発生等の任意の手段を用いて、パラメータ p_i と l_i の値をそれぞれ $0 \leq p_i \leq L$ および $l_{\min} \leq l_i \leq l_{\max}$ のようにコピー範囲を決定する。ここで、 L は個人識別子 O I D の全長であり、 l_{\min} および l_{\max} は $0 < l_{\min} < l_{\max} < L$ が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子 O I D の先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにコピー範囲を設定する。次に、図 10 (a), (b) に示すように、ペースト先頭位置を仮の役割識別子 A I D の先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにペースト位置を設定する。

【0038】

それから、図 10 (a), (b) に示すように、上述したコピー範囲の文字列を仮の役割識別子 A I D の上述したペースト位置に上書きして複写する（ステップ S 9 1 5）。このように上書きした文字列の特定の位置に位置情報 p_i および l_i の値を、CA が定めた方法で暗号化して、図 10 (c) で指定した位置に付加し（ステップ S 9 1 7）、更にこの位置情報を付加した文字列にセキュア・コミュニケーション・サービス S C S のホスト O I D（ホスト名、ドメイン名、または I P アドレス）を図 10 (c) に示すように付加する（ステップ S 9 1 9）。そして、このようにセキュア・コミュニケーション・サービス S C S のホスト O I D を付加した文字列に認証局 C A の O I D 秘密鍵で電子署名を施す（ステップ S 9 2 1）。

【0039】

次に、役割識別子 A I D による個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービス A D S 7 において、個人情報を登録するまでの流れを図 11 (a) に示す。同図に示すように、登録者であるユーザ B 3 は自らの役割識別子 A I D、移転制御情報、有効期限、および、性別、年齢、趣味等のプライバシー情報をアノニマス・ディレクトリ・サービス A D S 7 に送付す

る。

【0040】

また、アノニマス・ディレクトリ・サービスADS7における検索処理を図11(b)に示す。検索者であるユーザA3は、自らの役割識別子AIDと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスADS7に送信する。アノニマス・ディレクトリ・サービスADS7は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子AIDを抽出する。アノニマス・ディレクトリ・サービスADS7は最後に検索者の役割識別子AIDと検索条件にマッチした登録者の役割識別子AIDから個別化アクセスチケットPATを生成し、検索者であるユーザA3に交付する。

【0041】

個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスADS7の検索結果として生成する。

【0042】

次に、図12のフローチャートを参照して、ADSにおけるPAT生成処理について説明する。

【0043】

1. 検索者AID秘密鍵で署名された検索者AIDを入力する(ステップS1210)。

【0044】

2. ステップS1210における検索者AIDをその検索者AIDの公開鍵で認証する(ステップS1211)。

【0045】

3. ステップS1211における認証の結果

- ・ 検索者AIDが改竄されている場合処理を中止する。
- ・ 検索者AIDが改竄されていない場合、ステップS1215に進む。

【0046】

4. ステップS1211で認証済みの検索者AIDを、登録者AID(ADS登

録時に登録者AIDの秘密鍵で認証済み)と連結する(ステップS1215)。

【0047】

5. ステップS1215で連結した、検索者AIDと登録者AIDからなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定する。また、発信者フラグを「0」と設定する(ステップS1217)。

【0048】

6. ステップS1217の結果に、ADSのOID秘密鍵で署名する(ステップS1219)。

【0049】

7. ステップS1219の結果(つまり、PAT)を、検索者AIDに送信する(ステップS1221)。

【0050】

なお、PATを受信した検索者は、ADSのOID公開鍵を用いて受信したPATを認証し、改竄されていないければ、これを検索者端末の記憶装置に記憶し、改竄されていれば、破棄します。この手順は、図6と同様である。

【0051】

次に、個別化アクセスチケットPATによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子AIDと実際の発信者を対応付けられるようにすることである。

【0052】

アノニマス・ディレクトリ・サービスADS7および着信者は、個別化アクセスチケットPATの移転制御フラグを設定することにより、発信者に番号通知させるか否かを選択させることができる。

【0053】

移転制御フラグを「1」に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われるため、着信者は発信者の役割識別子AIDと実際の発信者を対応付けることができる(発信者番号通知)。また、移転制御フラグを「0」に設定した場合には、着信者は発信者の役割識別子AIDと

実際の発信者を対応付けることができない（発信者番号非通知）。

【0054】

図14のフローチャートを参照して、SCSにおけるメール接続制御の処理手順について説明する。

【0055】

1. メールを入力する（ステップS1411）。

【0056】

2. ステップS1411のメールのTo:フィールドからPATを抽出する。次に、このPATに対するADS公開鍵をADSに何らかの手段で問い合わせ、そのADS公開鍵を取得する。そして、PATをADS公開鍵で認証する（ステップS1413）。

【0057】

3. ステップS1413における認証の結果

- ・PATが改竄されている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する（ステップS1429）。

- ・PATが改竄されていない場合、ステップS1417に進む。

【0058】

4. ステップS1411のメールのFrom:フィールドから発信者AIDを抽出する。また、メールのTo:フィールドのPATの移転制御フラグを解析し、PATから発信者AIDを抽出する（ステップS1417, S1419）。

【0059】

5. ステップS1417, S1419で抽出した発信者AID同士を比較する（ステップS1421）。

【0060】

6. ステップS1421における比較の結果

- ・両者が一致しない場合ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する（ステップS1429）。

- ・両者が一致する場合、ステップS1425に進む。

【0061】

7. ステップS1411のメールのTo:フィールドのPATから有効期限を抽出する(ステップS1425)。

【0062】

8. ステップS1411のメールのTo:フィールドのPATが有効期限内かどうかを検証する。

【0063】

9. ステップS1421における検証の結果

- ・有効期限を過ぎている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する(ステップS1429)。

- ・有効期限内の場合、ステップS1431に進む。

【0064】

10. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を調べる。

【0065】

11. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を抽出する(ステップS1431)。

【0066】

12. ステップS1431における抽出の結果

- ・移転制御フラグ値が「1」の場合、図15～図17の手順に従い、移転制御を行ってから(ステップS1435)、図18の手順に従い、メールを着信者AID宛に転送する(ステップS1437)。

- ・移転制御フラグ値が「0」の場合、図18の手順に従い、メールを着信者AID宛に転送する(ステップS1437)。

【0067】

この移転制御について図15～図17を参照して説明する。まず、図15において、セキュア・コミュニケーション・サービスSCS5は、個別化アクセスチ

ケットPATを入力すると（ステップS1511）、それから、セキュア・コミュニケーション・サービスSCS5は、任意の文字列、例えばタイムスタンプを生成し（ステップS1517）、この生成した文字列を発信者の役割識別子AIDに送信する（ステップS1519）。

【0068】

ユーザにおいては、図16に示すように、前記文字列を受信すると（ステップS1611）、この文字列に発信者役割識別子AIDの秘密鍵で署名し（ステップS1613）、署名つき該文字列をセキュア・コミュニケーション・サービスSCS5に送信する（ステップS1615）。

【0069】

セキュア・コミュニケーション・サービスSCS5においては、図17に示すように、署名つき前記文字列を受信すると（ステップS1711）、発信者の役割識別子AIDの公開鍵で認証し（ステップS1713）、改竄されているか否かをチェックする（ステップS1715）。改竄されている場合には、改竄されている旨を何らかの手段で発信者AIDに通知してからアボート（異常終了）するが（ステップS1717）、改竄されていない場合には、セキュア・コミュニケーション・サービスSCS5は、図18に示す接続制御を行う。

【0070】

以下、図18のフローチャートを参照して接続制御について説明する。

【0071】

1. メールのTo:フィールドのPATから、発信者のSCSホストOIDと着信者のSCSホストOIDを抽出する（ステップS1811）。

【0072】

2. ステップS1811で抽出した発信者、着信者それぞれのSCSホストOIDのデータ形式を調べる（ステップS1813）。

【0073】

3. ステップS1813における調査の結果

・発信者SCSホストOIDと着信者SCSホストOIDのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップS18

15に進み、ホスト名またはドメイン名で与えられているSCSホストOIDをDNS (Domain Name Service) に問い合わせ、そのホスト名またはドメイン名に対するIPアドレスを取得してから、ステップS1817に進む。

・発信者SCSホストOIDと着信者SCSホストOIDがともにIPアドレスで与えられている場合には、そのままステップS1817に進む。

【0074】

4. ステップS1815, S1817で抽出あるいは変換したIPアドレスを比較する(ステップS1817)。

【0075】

5. ステップS1817における比較の結果

・発信者SCSホストOID (IPアドレス) と着信者SCSホストOID (IPアドレス) が一致する場合、ステップS1819からステップS1823に進み、発信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する(ステップS1823)。この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1825からステップS1827に進み、ステップS1811のメールを、メールのFrom: フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0076】

また、ステップS1825において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、着信者AIDを検索条件として、着信拒否データベースに問い合わせる(ステップS1829)。

【0077】

この問い合わせの結果、メールのTo: フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1831からステップS1827に進み、メールを、メールのFrom: フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0078】

また、ステップS1831において、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納して正常終了する(ステップS1833)。

【0079】

一方、ステップS1819において、発信者SCSホストOID(IPアドレス)と着信者SCSホストOID(IPアドレス)が一致しない場合、について説明する。

【0080】

まず、SMTPに従い、メールを着信者AIDをアカウントに持つSCSホストに転送する(ステップS1835)。

【0081】

次に、着信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する(ステップS1837)。

【0082】

この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1839からステップS1841に進み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0083】

また、ステップS1839において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、ステップS1843に進む。ステップS1843では着信者AIDを検索条件として、着信拒否データベースに問い合わせる。

【0084】

ステップS1843における問い合わせの結果、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1845からステップS1841に進

み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0085】

また、ステップS1845において、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されていない場合、ステップS1847に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【0086】

図19のフローチャートを参照して、SCSにおけるメール返信処理について説明する。

【0087】

1. エラーを検出したSCSホストは、PAT<エラーを検出したSCSホストOID|From:フィールドの発信者AID>を生成する(ステップS1911)。

【0088】

2. ステップS1911のSCSホストは、ステップS1911で生成したPATを、エラーが発生したメールのTo:フィールドにセットする(ステップS1913)。

【0089】

3. ステップS1911のSCSホストは、ステップS1913でセットしたメールを(発信者AID宛に)送信する(ステップS1915)。

【0090】

次に、個別化アクセスチケットPATに対する着信拒否について説明する。

【0091】

着信者AID側で指定した個別化アクセスチケットPATがTo:フィールドに記述されたメールが、着信者AIDに含まれるホストOIDのセキュア・コミュニケーション・サービスSCS5に到着した場合には、そのセキュア・コミュニケーション・サービスSCS5はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者AID宛に返信する。この一連の処理を着信拒否

と呼ぶ。

【0092】

ユーザにおける着信拒否申請処理について図22に示すフローチャートを参照して説明する。ユーザは役割識別子AIDと個別化アクセスチケットPATを入力し（ステップS2211）、図24の上側に示す着信拒否申請メッセージを作成し（ステップS2213）、着信者AIDの秘密鍵で署名、暗号化する（ステップS2215）。それから、着信者はこの暗号化した申請メッセージをセキュア・コミュニケーション・サービスSCS5に送信する（ステップS2217）。

【0093】

着信拒否申請メッセージは、図24の上側に示すように、着信者の役割識別子AIDと申請項目から構成される。申請項目は次の2種類のうちのいずれかである。

(1) 着信拒否の設定

<着信者AIDの実体>REFUSE<PATの実体、IPアドレス、ドメイン名、ホスト名>

(2) 着信拒否の解除

<着信者AIDの実体>RECONNECT <PATの実体、IPアドレス、ドメイン名、ホスト名>

【0094】

次に、図23に示すフローチャートを参照して、セキュア・コミュニケーション・サービスSCS5における着信拒否設定処理について説明する。セキュア・コミュニケーション・サービスSCS5は、着信拒否申請メッセージを受け取ると（ステップS2311）、着信者のAID公開鍵で認証し（ステップS2313）、改竄されているか否かをチェックする（ステップS2315）。改竄されていない場合には、着信拒否メッセージから個別化アクセスチケットPAT、IPアドレス、ドメイン名、またはホスト名を抽出し、該個別化アクセスチケットPAT、該IPアドレス、該ドメイン名、該ホスト名を着信拒否データベース（DB）に登録（または削除）する（ステップS2317）。それから、図24の

下側に示すような着信拒否通知メッセージを生成し（ステップ S 2 3 1 9）、着信者 A I D 公開鍵で署名、暗号化し（ステップ S 2 3 2 1）、この暗号化されたメッセージを着信者 A I D に返信する（ステップ S 2 3 2 3）。

【0095】

着信拒否通知メッセージは、図 2 4 の下側に示すように、着信者の役割識別子 A I D と処理結果から構成されている。処理結果は次に示す 2 種類のうちのいずれかである。

(1) 着信拒否の設定結果

＜着信者 A I D の実体＞REFUSE＜成功 | 失敗＞＜P A T の実体、I P アドレス、ドメイン名、ホスト名＞

(2) 着信拒否の解除結果

＜着信者 A I D の実体＞RECONNECT ＜成功 | 失敗＞＜P A T の実体、I P アドレス、ドメイン名、ホスト名＞

【0096】

着信拒否の実行に当たっては、セキュア・コミュニケーション・サービス S C S 5 は、個別化アクセスチケット P A T を着信拒否データベースに問い合わせる。該当個別化アクセスチケットが存在する場合、または、発信者 A I D に、該当する I P アドレス、ホスト名、ドメイン名が含まれる場合には、メールを発信者 A I D に返信する。存在しない場合には、メッセージを着信者アカウントのメールボックスまたはスプールに格納する。

【0097】

図 2 5 のフローチャートを参照して、同一性の判定について説明する。

【0098】

1. 変数 $O I D_M$ の初期値を、 $O I D$ の全長 L と等しい長さで、かつ、すべての値が 0 であるビット列と定義する。また、変数 $O I D_V$ の初期値を、 $O I D$ の全長 L と等しい長さで、かつ、すべての値が 0 であるビット列と定義する（ステップ S 2 5 1 1）。

【0099】

2. 処理対象の A I D の集合から 1 個の A I D を選択し、以下のビット演算を実

行する（ステップ S 2 5 1 3）。

【0100】

(a) A I D に含まれる位置情報をもとにして、変数 A I D_M と変数 A I D_V の値を決定する（ステップ S 2 5 1 5）。ここで、

- ・ A I D_M は O I D の全長 L と等しい長さで、かつ、
 - － O I D 情報が定義されている位置の値は 1 である。
 - － O I D 情報が定義されていない位置の値は 0 である。
- ビット列と定義する（図 2 6）。

【0101】

- ・ A I D_V は O I D の全長 L と等しい長さで、かつ、
 - － O I D 情報が定義されている位置の値は O I D 情報の実際の値である
 - － O I D 情報が定義されていない位置の値は 0 である
- ビット列と定義する（図 2 6）。

【0102】

(b) O I D_M と A I D_M の AND 演算を実行し、その結果を変数 O V R_M に代入する（ステップ S 2 5 1 7）。

【0103】

(c) O V R_M と A I D_M の AND 演算と、O V R_M と O I D_M の AND 演算を実行し、その演算結果を比較する（ステップ S 2 5 1 9）。

・ 一致する場合 O I D_M と A I D_M の OR 演算を実行し、実行結果を O I D_M に代入する（ステップ S 2 5 2 1）。また、O I D_V と A I D_V の OR 演算を実行し、実行結果を O I D_M に代入する（ステップ S 2 5 2 3）。

- ・ 一致しない場合、ステップ S 2 5 2 5 に進み、実行する。

【0104】

(d) 処理対象の A I D の集合から、次に処理する A I D を抽出する。

・ 集合に少なくとも 1 個の A I D が含まれている場合、ステップ S 2 5 1 9 を実行する。

- ・ 集合に A I D が 1 個も含まれていない場合、ステップ S 2 5 2 7 に進む。

【0105】

(e) $O I D_M$ および $O I D_V$ の値を出力する（ステップ S2527）。

【0106】

最終的に得られた $O I D_M$ の値は、処理対象の $A I D$ の集合から復元できた $O I D$ 情報のすべての位置を表している。また、最終的に得られた $O I D_V$ の値は、処理対象の $A I D$ の集合から復元できた $O I D$ 情報のすべてを表している。つまり、 $O I D_M$ と $O I D_V$ の値を用いると、

(a) $O I D_V$ の値を検索条件とすると、確率的にはあるが $O I D$ を求めることができる。

【0107】

(b) 上記検索の精度を、 $O I D$ 全長 L との比 $O I D_M / L$ で定量的に評価することができる。

【0108】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子 $O I D$ からこれらの情報を隠蔽した役割識別子 $A I D$ を作成すべく図 7 に示すような役割識別子 $A I D$ 請求メッセージを作成し、認証局 $C A 1$ に送信すると、認証局 $C A 1$ は、該メッセージを受け取って、役割識別子 $A I D$ を生成し、ユーザに交付する。

【0109】

ユーザは、この交付された役割識別子 $A I D$ および性別、年齢、趣味等の個人情報情報をアノニマス・ディレクトリ・サービス $A D S 7$ に送信し、アノニマス・ディレクトリ・サービス $A D S 7$ に役割識別子 $A I D$ と個人情報情報を登録する。このように登録された情報を検索する場合は、検索者は自己の役割識別子 $A I D$ と検索条件（性別、年齢、趣味等のプライバシー情報）をアノニマス・ディレクトリ・サービス $A D S 7$ に送信する。アノニマス・ディレクトリ・サービス $A D S 7$ は、これらの情報を受信すると、該検索条件にマッチした登録者の役割識別子 $A I D$ を抽出する。そして、アノニマス・ディレクトリ・サービス $A D S 7$ は、検索者の役割識別子 $A I D$ と検索条件にマッチした登録者の役割識別子 $A I D$ から個別化アクセスチケット $P A T$ を生成し、検索者に交付する。

【0110】

この個別化アクセスチケットPATには、図3(c)に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【0111】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者AIDと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを1に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われ、着信者は発信者AIDと実際の発信者を対応付けることができる（発信者番号通知）。また、該フラグを0に設定した場合は、移転制御は行われず、着信者は発信者AIDと実際の発信者を対応付けることはできない（発信者番号非通知）。

【0112】

また、個別化アクセスチケットPATで着信者を指定した呼を個別化アクセスチケットPAT内で定義した着信者役割識別子AIDまたは発信者役割識別子AIDに着信するように、通信網に対して接続要求をすることができる。更に、個別化アクセスチケットPATで指定した呼のうち、着信者が選択した個別化アクセスチケットPATの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子AIDで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子AIDから個人識別子OIDの同一性を判定することができ、かつ、その個人識別子のある確率で取り出すことができる。

【0113】

【発明の効果】

以上説明したように、本発明によれば、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む個別化アクセスチケットを発

行し、役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名を用いて、個別化アクセスチケットが改竄されていない、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという3要件を検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、従来のような第三者からの攻撃等を的確に防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。

【図面の簡単な説明】

【図1】

本発明において使用される役割識別子AID、個別化アクセスチケットPATを示す説明図である。

【図2】

本発明の一実施形態の全体構成図である。

【図3】

個人識別子OIDと役割識別子AIDの例を示している。

【図4】

ユーザが役割識別子AIDを認証局CAに対して請求する処理を示すフローチャートである。

【図5】

役割識別子AIDの請求に対する認証局CAが役割識別子AIDをユーザに対して交付する処理を示すフローチャートである。

【図6】

ユーザにおけるAID交付処理を示すフローチャートである。

【図7】

役割識別子AIDの請求メッセージの例を示す図である。

【図 8】

役割識別子 A I D の交付メッセージの例を示す図である。

【図 9】

認証局 C A における役割識別子 A I D の生成処理を示すフローチャートである。

【図 10】

図 9 の A I D 生成処理に関連する説明図である。

【図 11】

アノニマス・ディレクトリ・サービス A D S における役割識別子 A I D の登録と個別化アクセスチケット P A T の交付の例を示す説明図である。

【図 12】

A D S において個別化アクセスチケット P A T を生成する場合の処理を示すフローチャートである。

【図 13】

図 12 の P A T 生成処理に関連する説明図である。

【図 14】

S C S におけるメール転送制御を示すフローチャートである。

【図 15】

S C S における移転制御を示すフローチャートである。

【図 16】

ユーザにおける移転制御を示すフローチャートである。

【図 17】

S C S における移転制御を示すフローチャートである。

【図 18】

S C S における個別化アクセスチケット P A T に対する接続制御を示すフローチャートである。

【図 19】

S C S におけるメール返信処理を示すフローチャートである。

【図 20】

ユーザ間の電子メールの例を示す図である。

【図 21】

着信拒否された場合の電子メールの例を示す図である。

【図 22】

ユーザにおける着信拒否申請処理を示すフローチャートである。

【図 23】

SCSにおける着信拒否設定処理を示すフローチャートである。

【図 24】

着信拒否申請メッセージおよび着信拒否通知メッセージの例を示す図である。

【図 25】

役割識別子 A I D について個人識別子 O I D の同一性を判定する処理を示すフローチャートである。

【図 26】

図 25 に示す同一性判定処理に関連する役割識別子 A I D および個人識別子 O I D の例を示す図である。

【図 27】

アナログ公衆網における二重番号登録を示す説明図である。

【図 28】

アナログ公衆網における発信者番号通知を示す説明図である。

【図 29】

デジタル携帯網およびアナログ公衆網における着信拒否を示す説明図である。

【図 30】

匿名電子メールの説明図である。

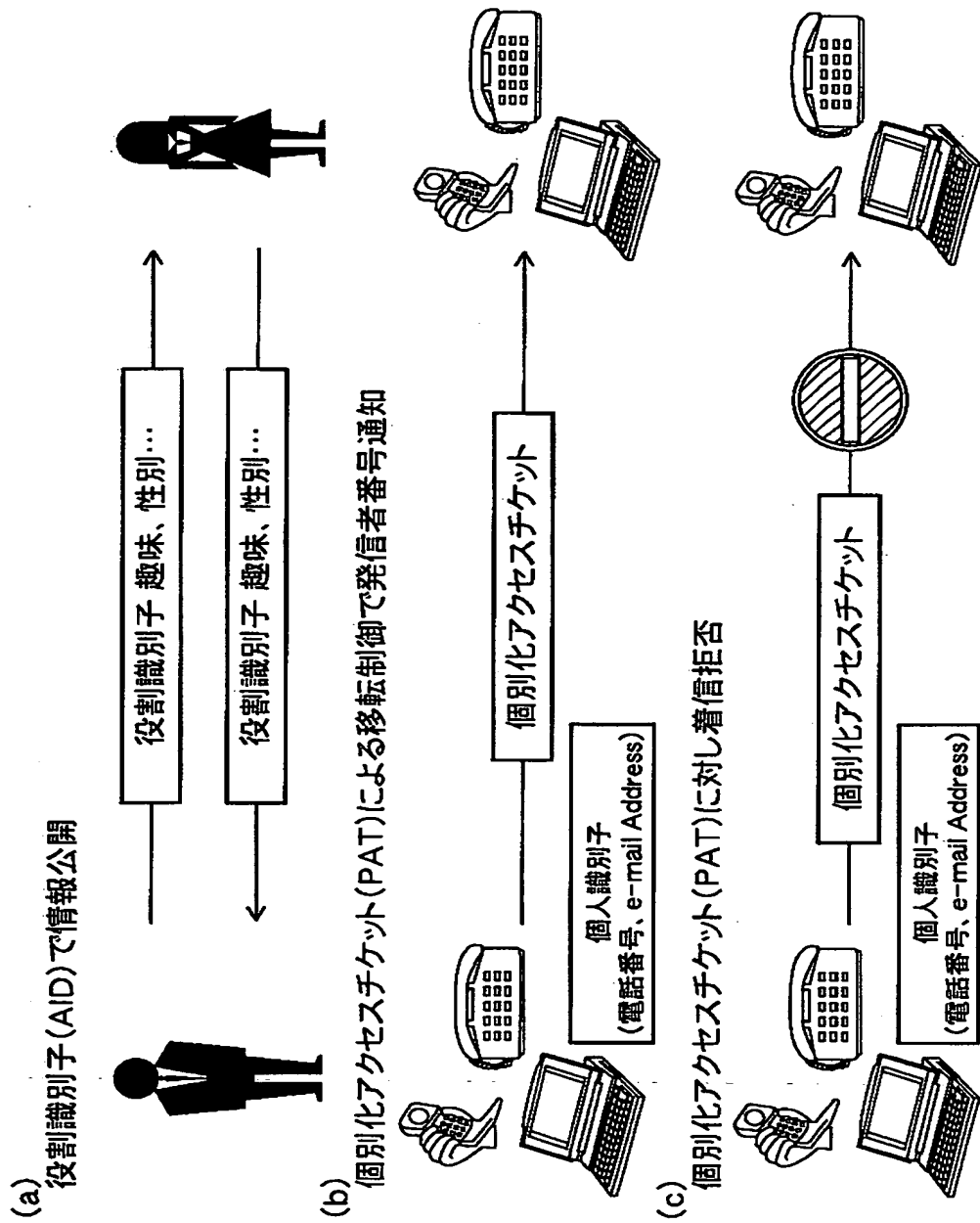
【符号の説明】

- 1 認証局 C A
- 3 ユーザ
- 5 セキュア・コミュニケーション・サービス S C S
- 7 アノニマス・ディレクトリ・サービス A D S

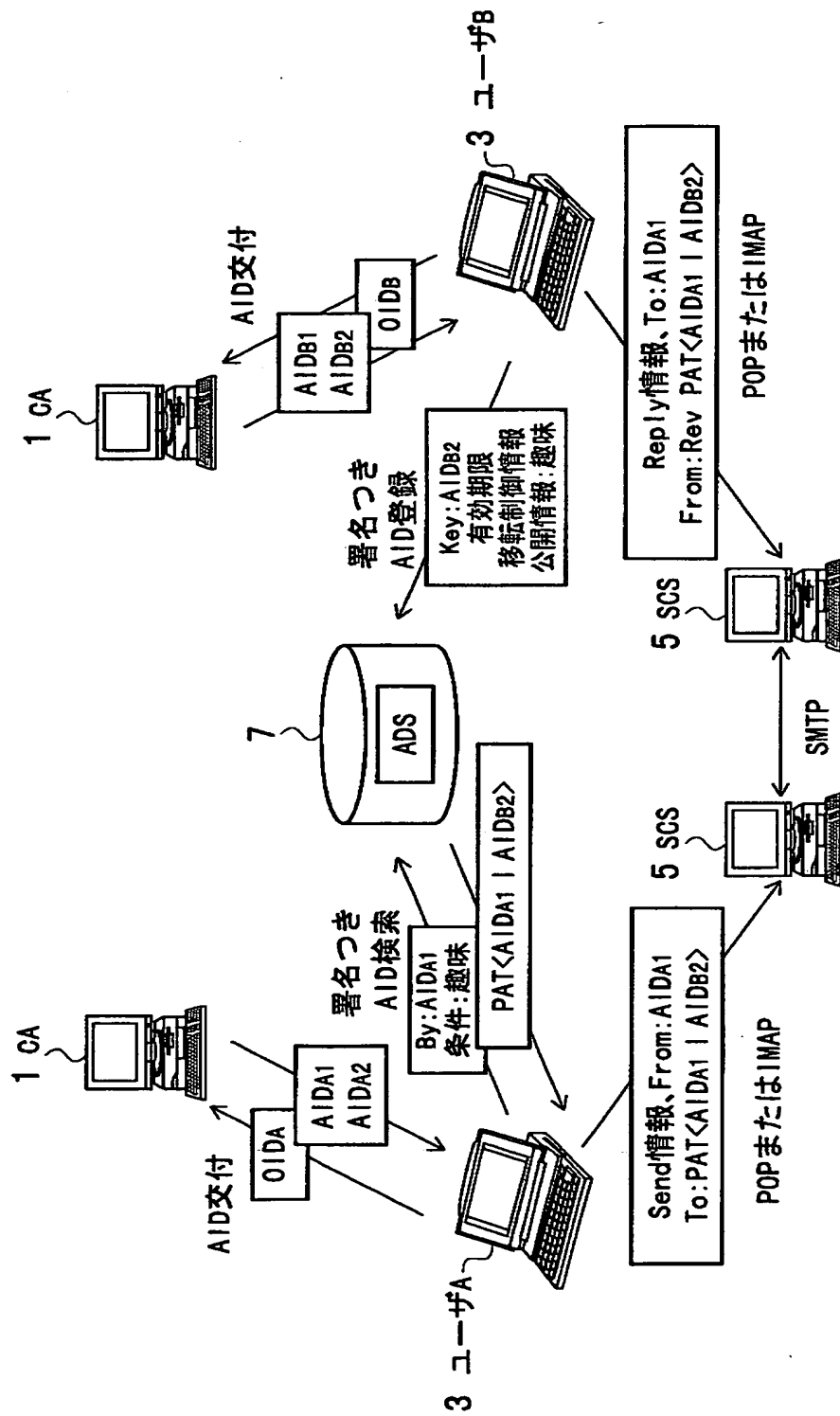
【書類名】

図面

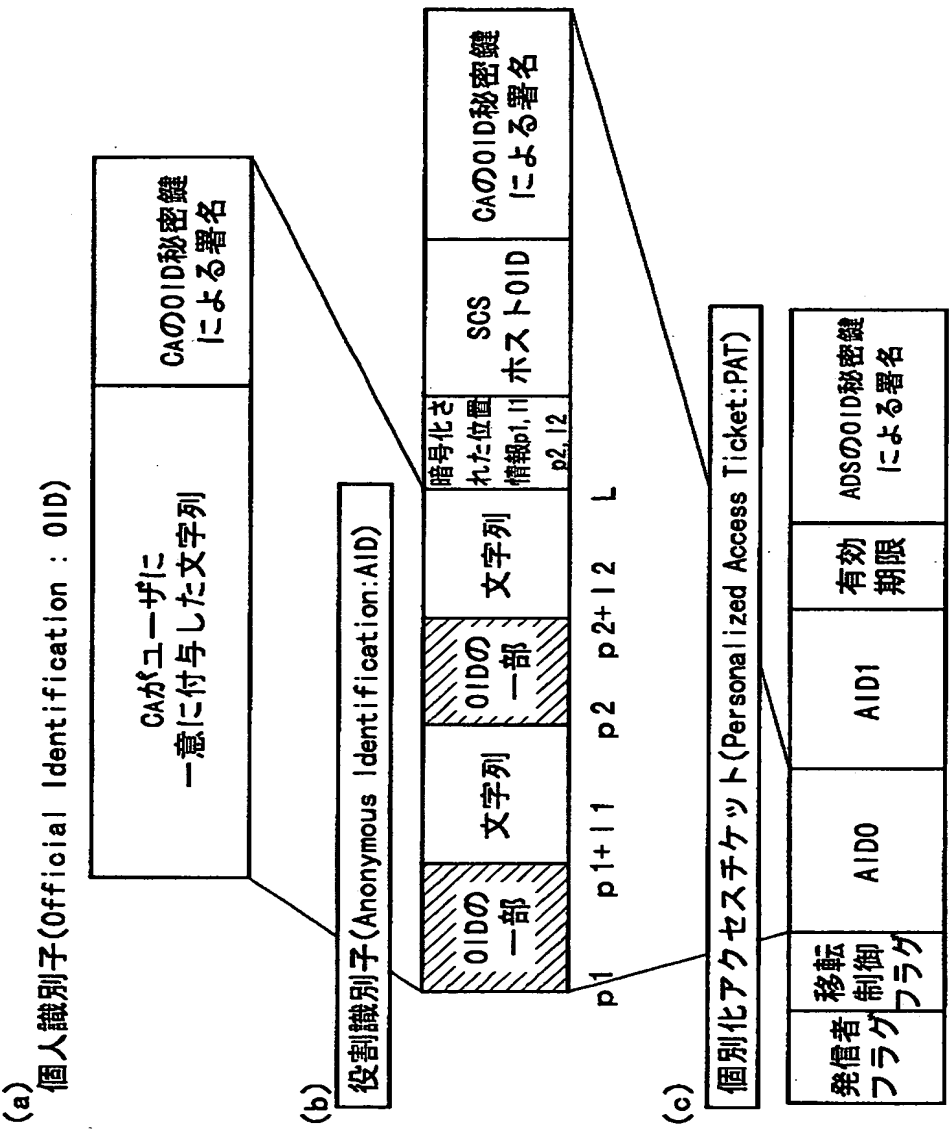
【図 1】



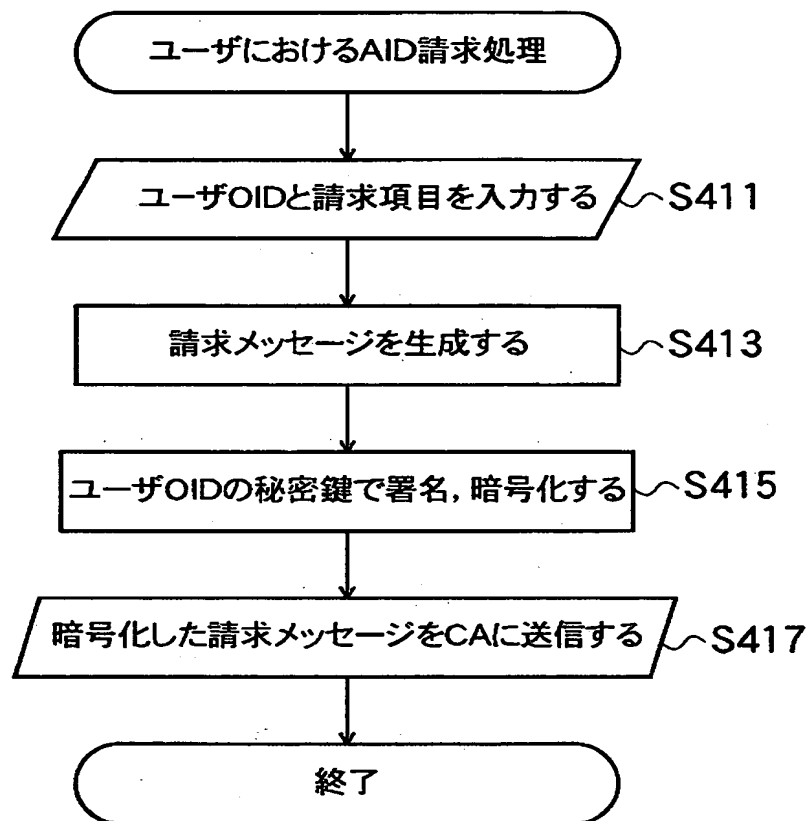
【図 2】



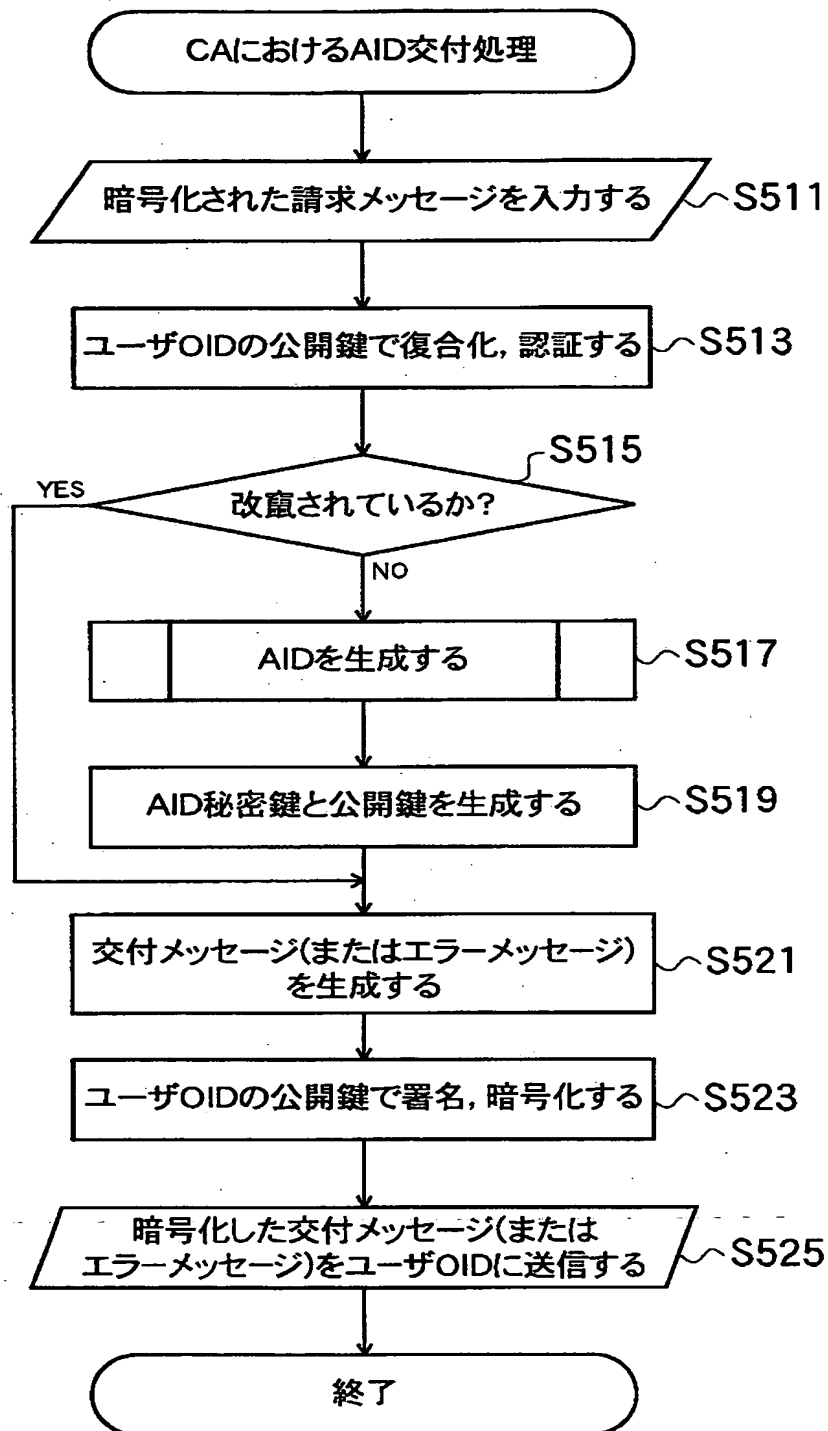
【図 3】



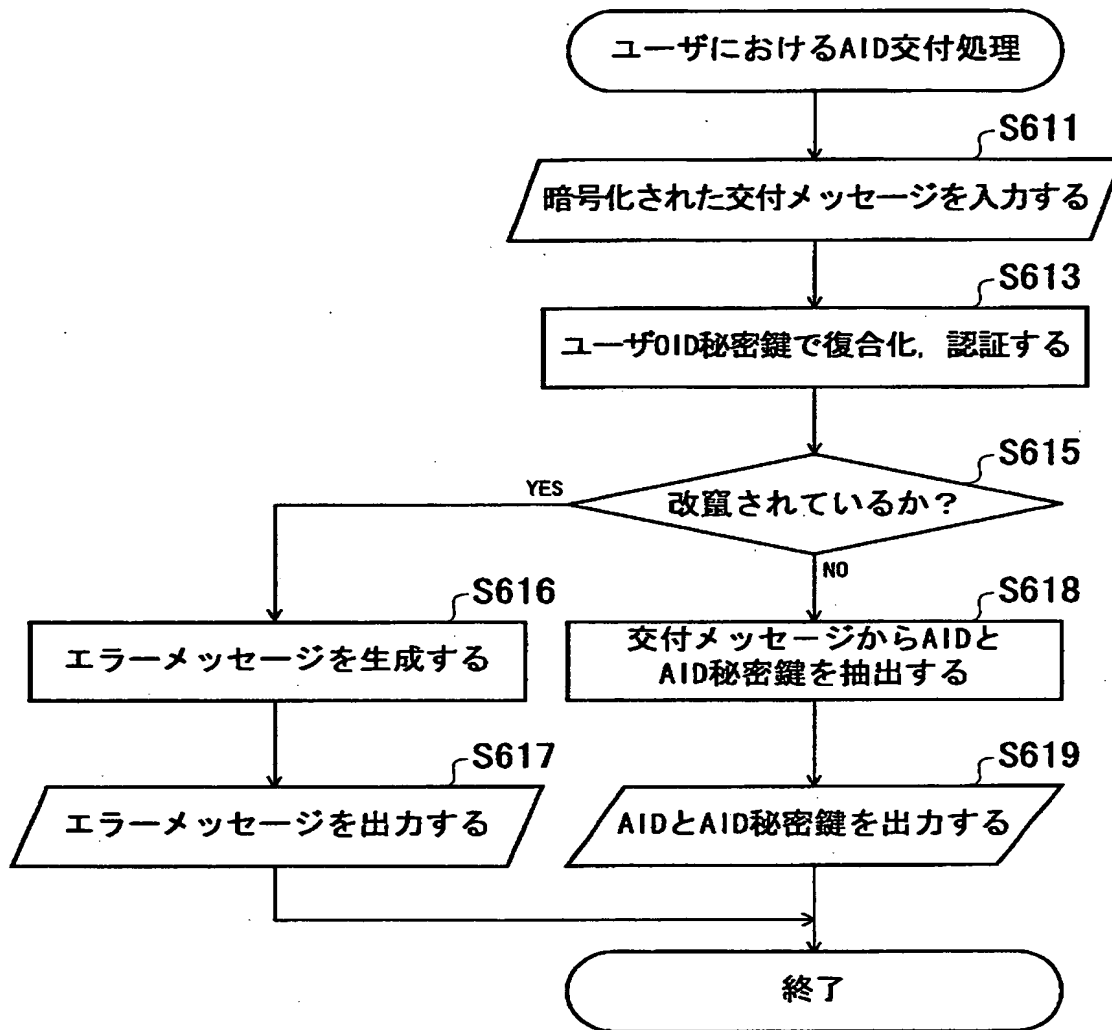
【図4】



【図 5】



【図 6】



【図 7】

AID請求メッセージの例

REQUEST AID 2

(新規AIDを2個請求する場合)

<ユーザOIDの秘密鍵による署名>

(送信時には、ユーザOIDの秘密鍵で暗号化する)

DISCARD AID AID1の実体 AID1の秘密鍵

DISCARD AID AID2の実体 AID2の秘密鍵

(既存AIDであるAID1とAID2を廃止したい場合)

<ユーザOID秘密鍵による署名>

(送信時には、ユーザOIDの秘密鍵で暗号化する)

【図 8】

AID交付メッセージの例

NEW AID AID3の実体 AID3の秘密鍵 OK

(新規AIDであるAID3は交付成功)

NEW AID NG

(交付失敗,つまり,エラーメッセージ)

<ユーザOIDの公開鍵による署名>

(送信時には、ユーザOIDの公開鍵で暗号化する)

DISCARD AID AID1の実体 OK

(既存AIDであるAID1は廃止成功)

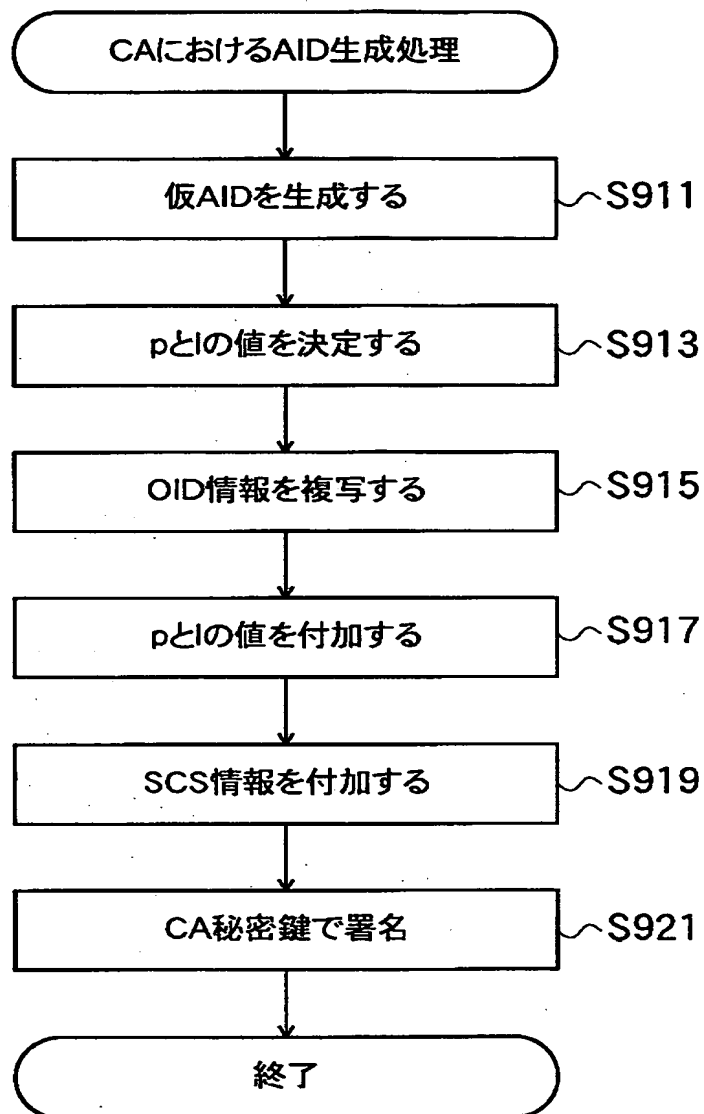
DISCARD AID AID2の実体 NG

(既存AIDであるAID2の廃止失敗のエラーメッセージ)

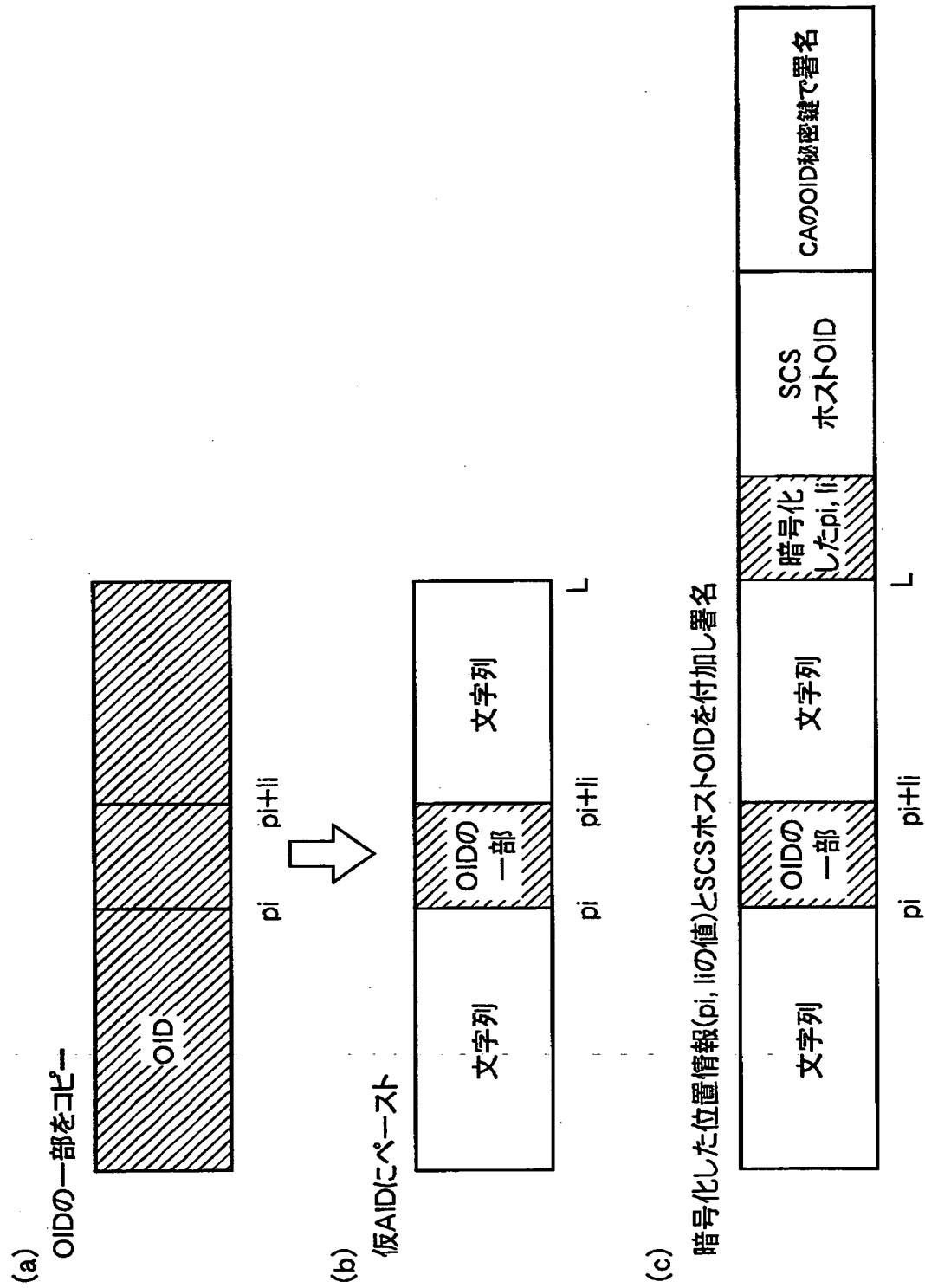
<ユーザOIDの公開鍵による署名>

(送信時には、ユーザOIDの公開鍵で暗号化する)

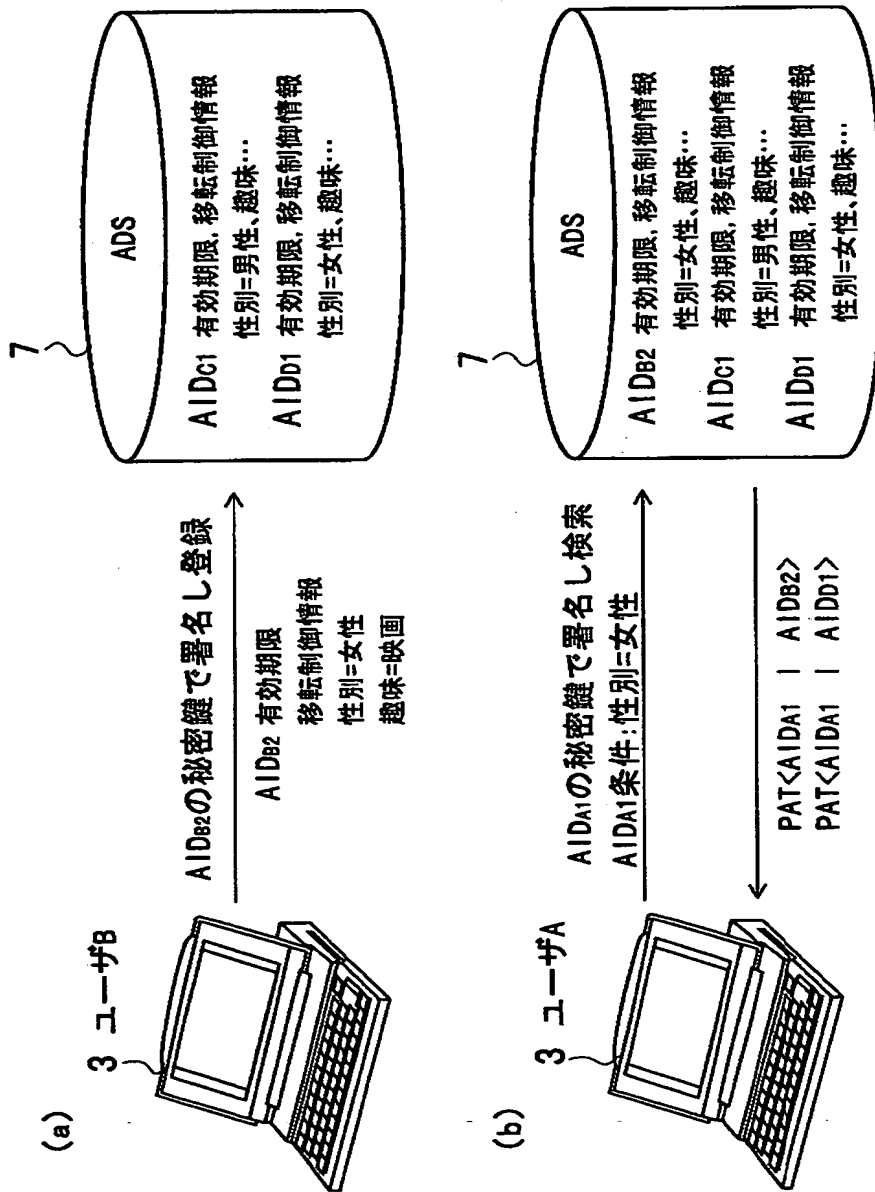
【図9】



【図 10】

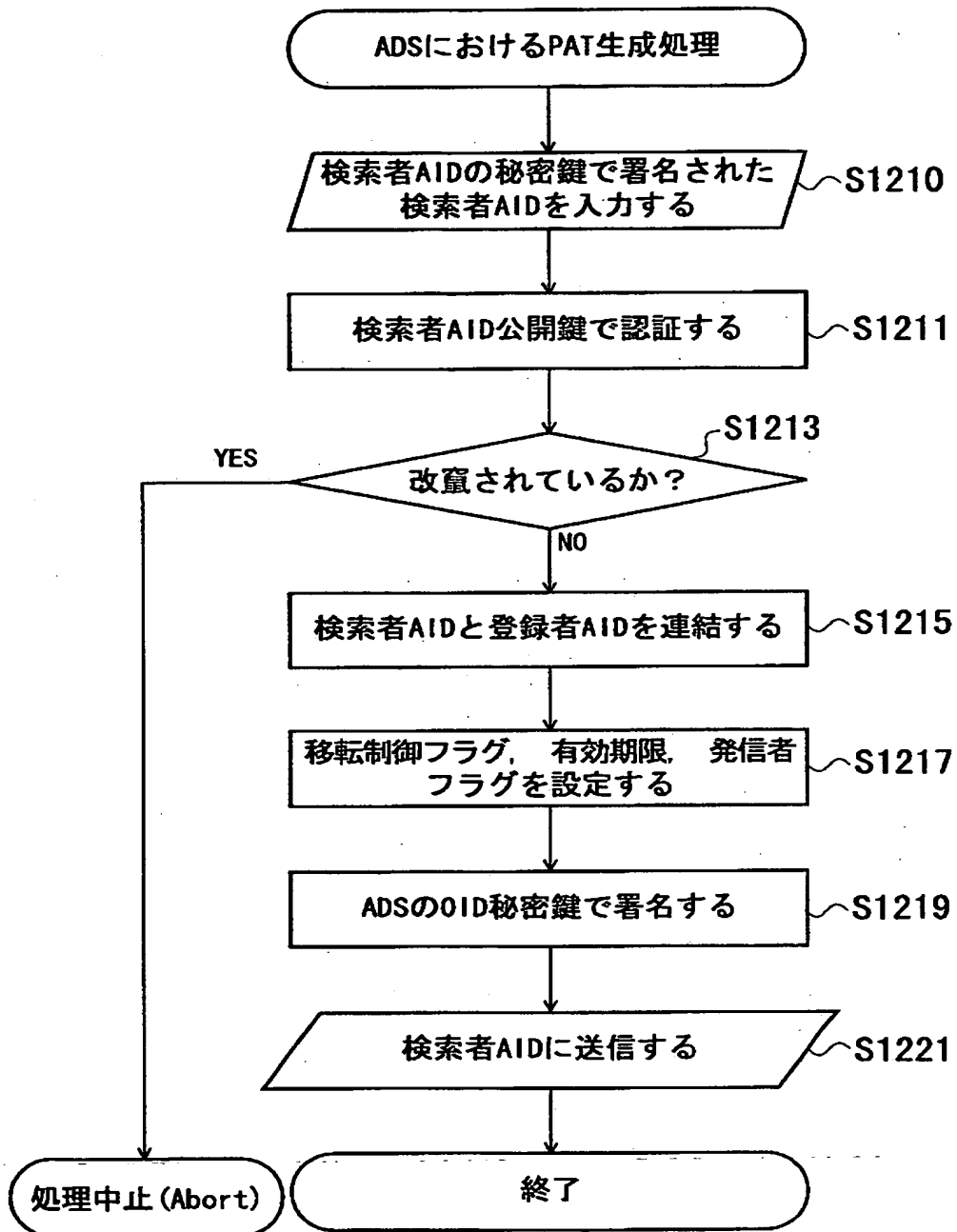


【図 11】

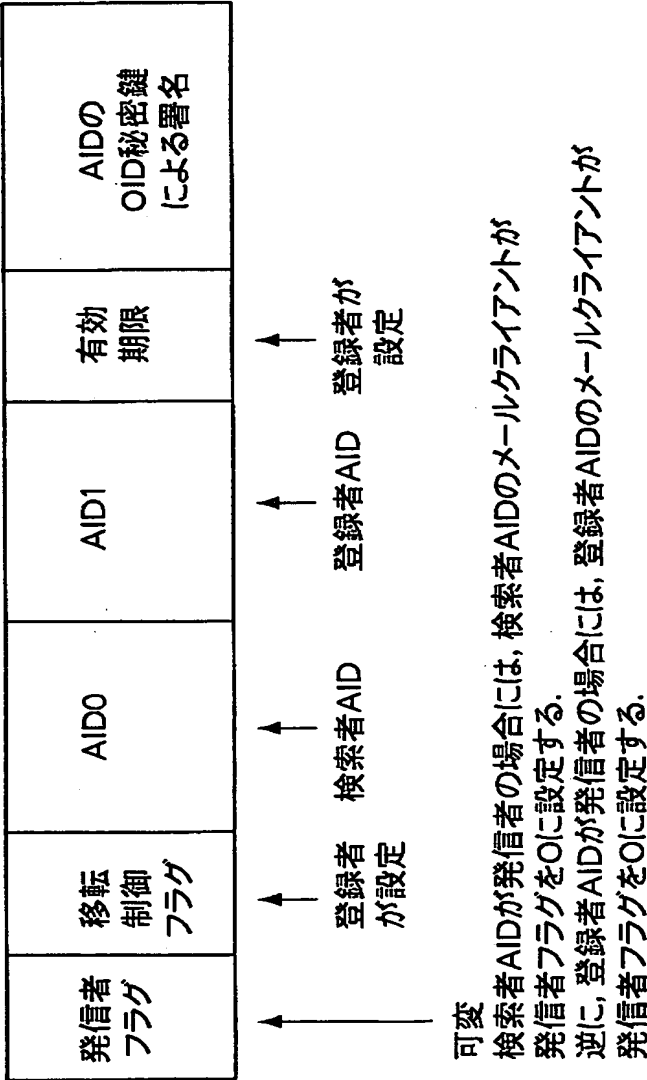


ADSのAID秘密鍵で署名、暗号化し交付

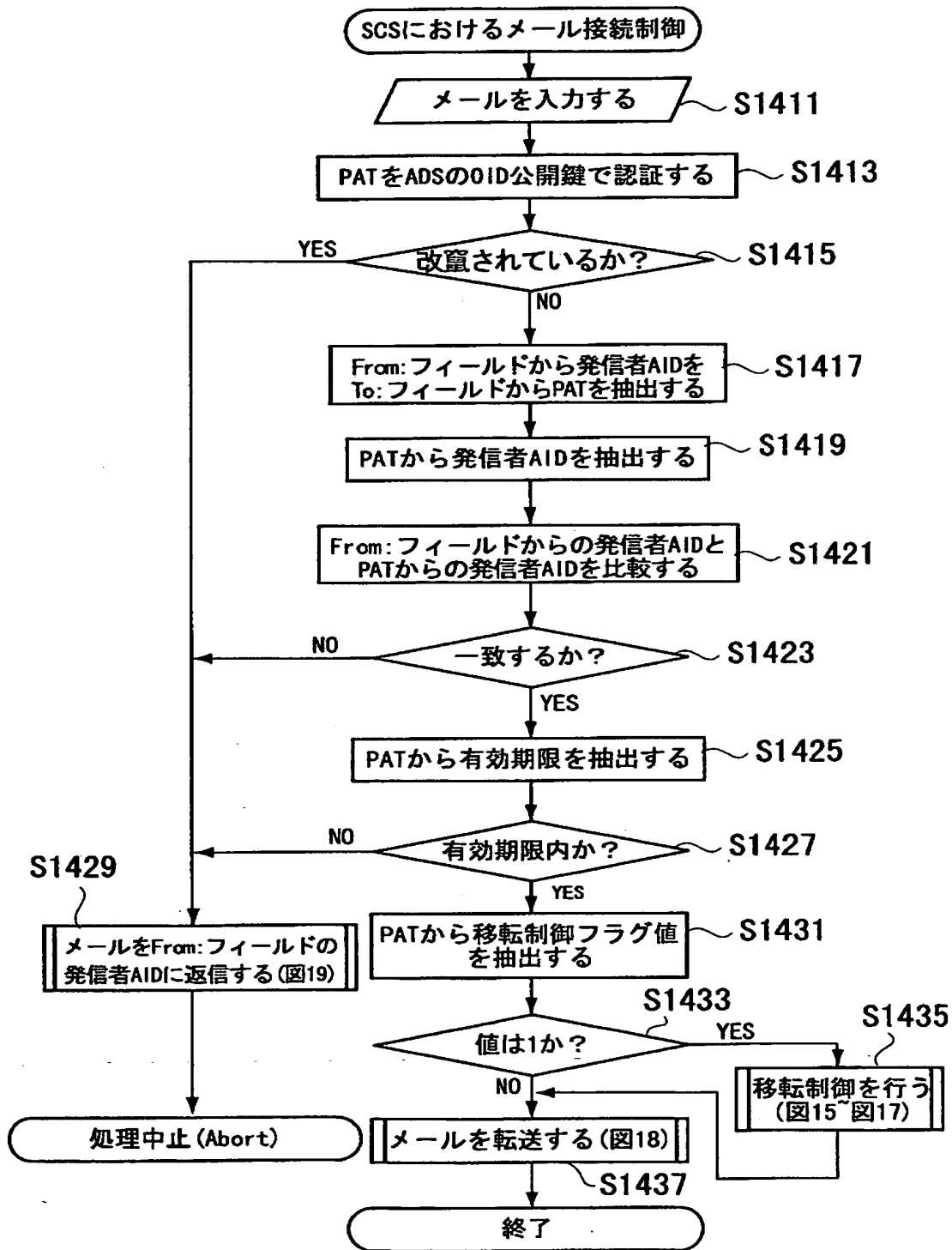
【図 12】



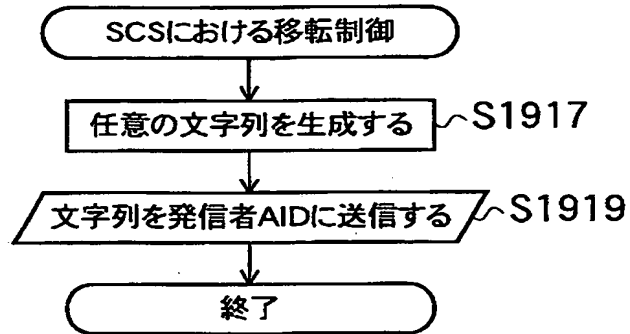
【図 13】



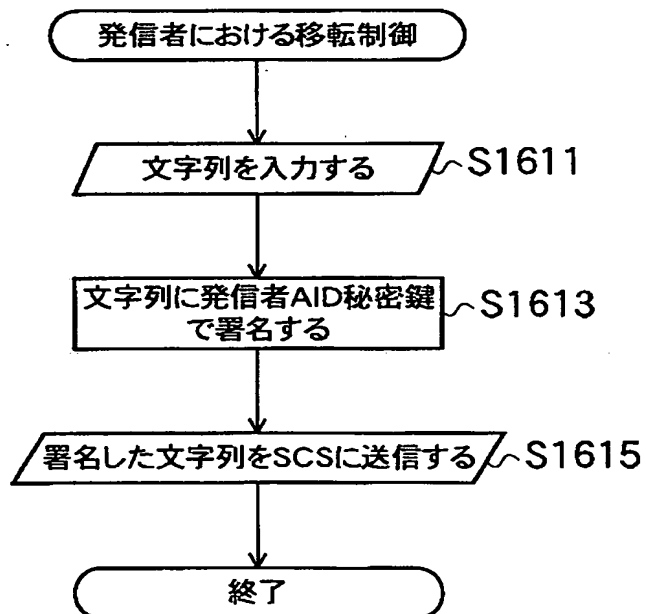
【図 14】



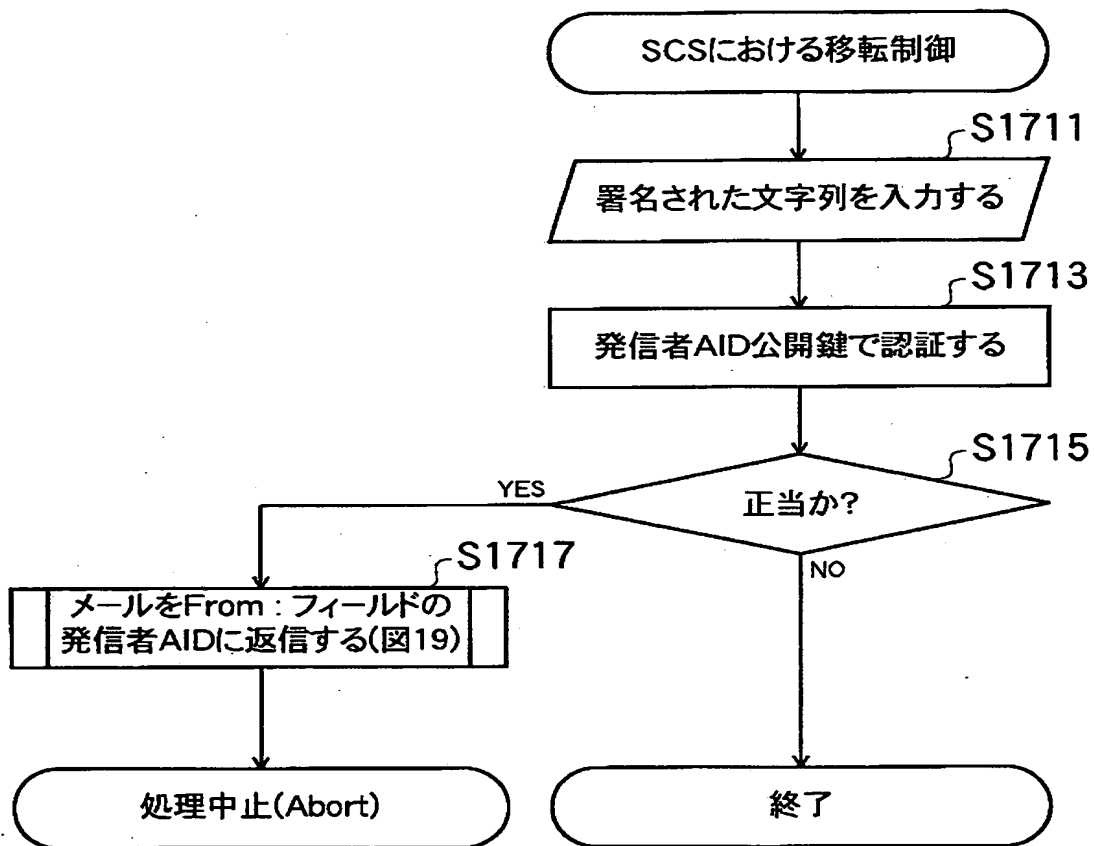
【図 15】



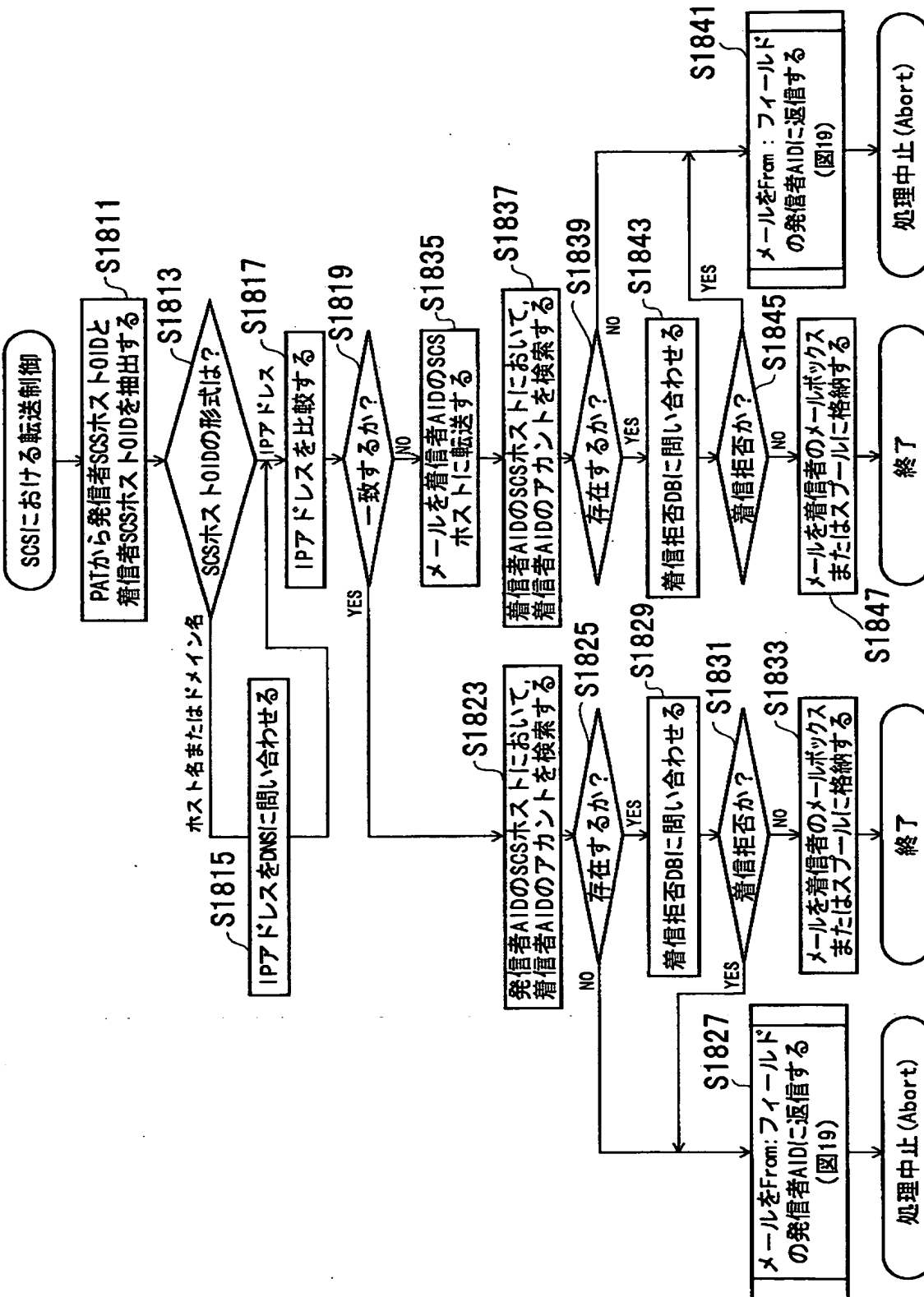
【図 16】



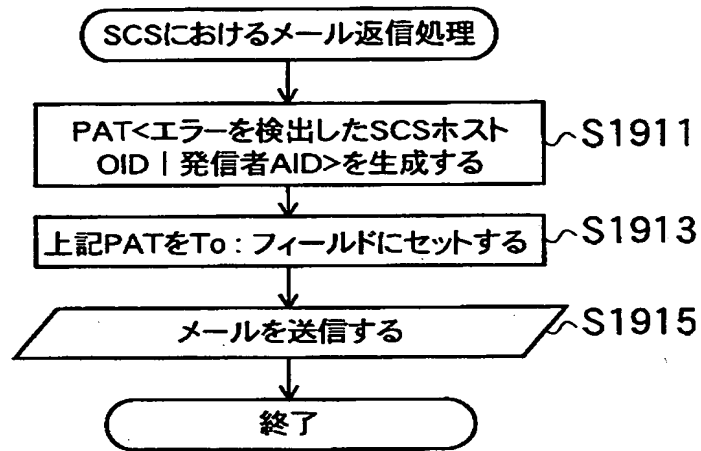
【図 17】



【図 18】



【図 19】



【図 20】

クライアント間の電子メールの例

送信

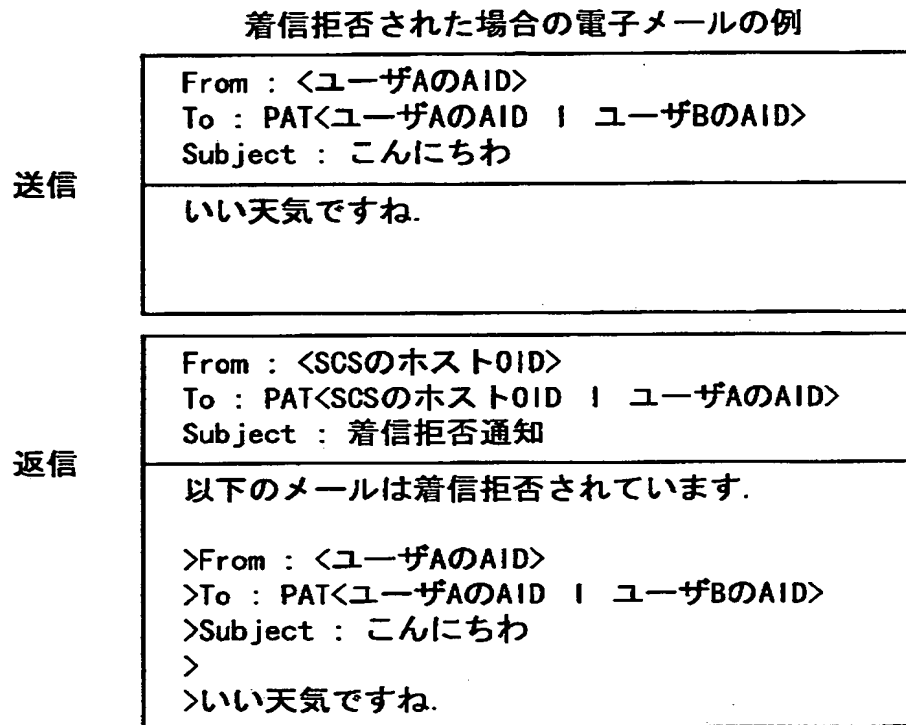
From : <ユーザAのAID> To : PAT<ユーザAのAID ユーザBのAID> Subject : こんにちは
いい天気ですね.

返信

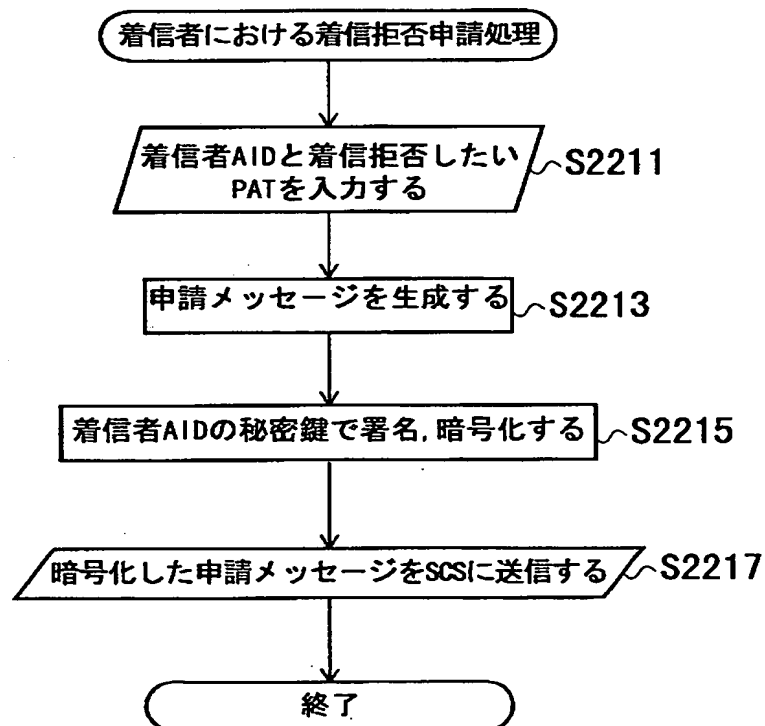
From : <ユーザBのAID> To : Rev PAT<ユーザAのAID ユーザBのAID> Subject : Re : こんにちは
そうですね.

PAT<A | B>は発信者フラグが0(つまり発信者はA)のPAT
Rev PAT<A | B>は発信者フラグが1(つまり発信者はB)のPAT

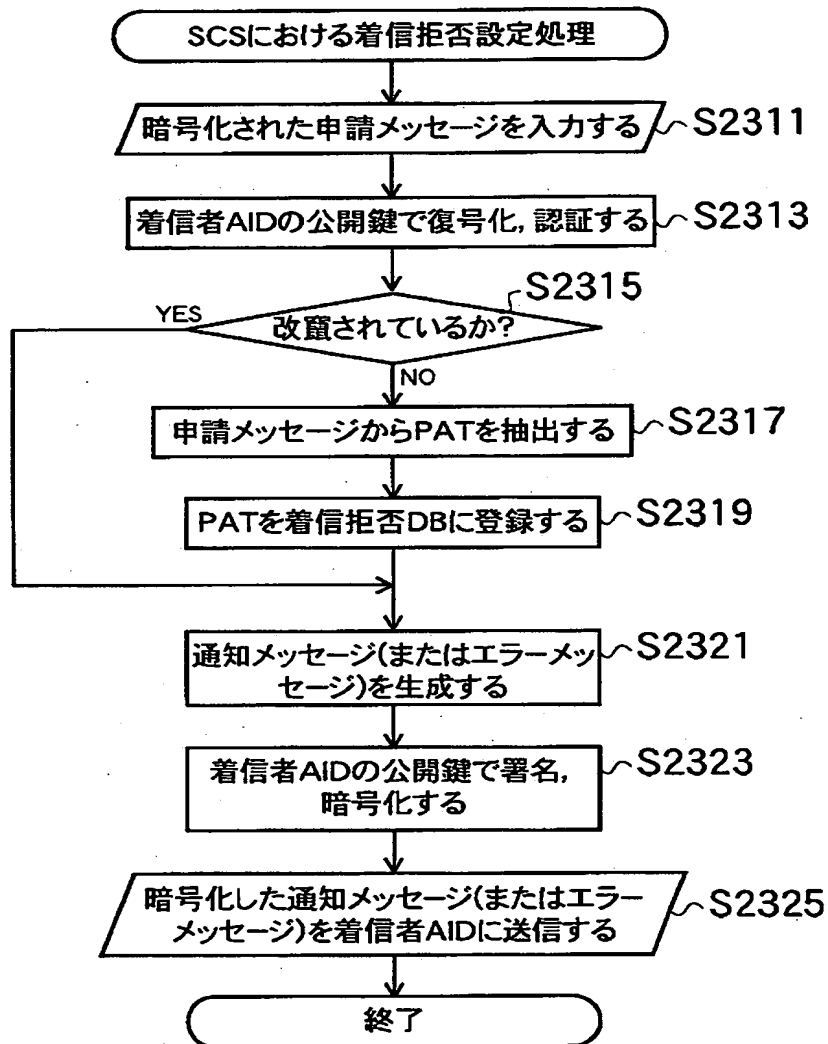
【図 21】



【図 22】



【図 23】



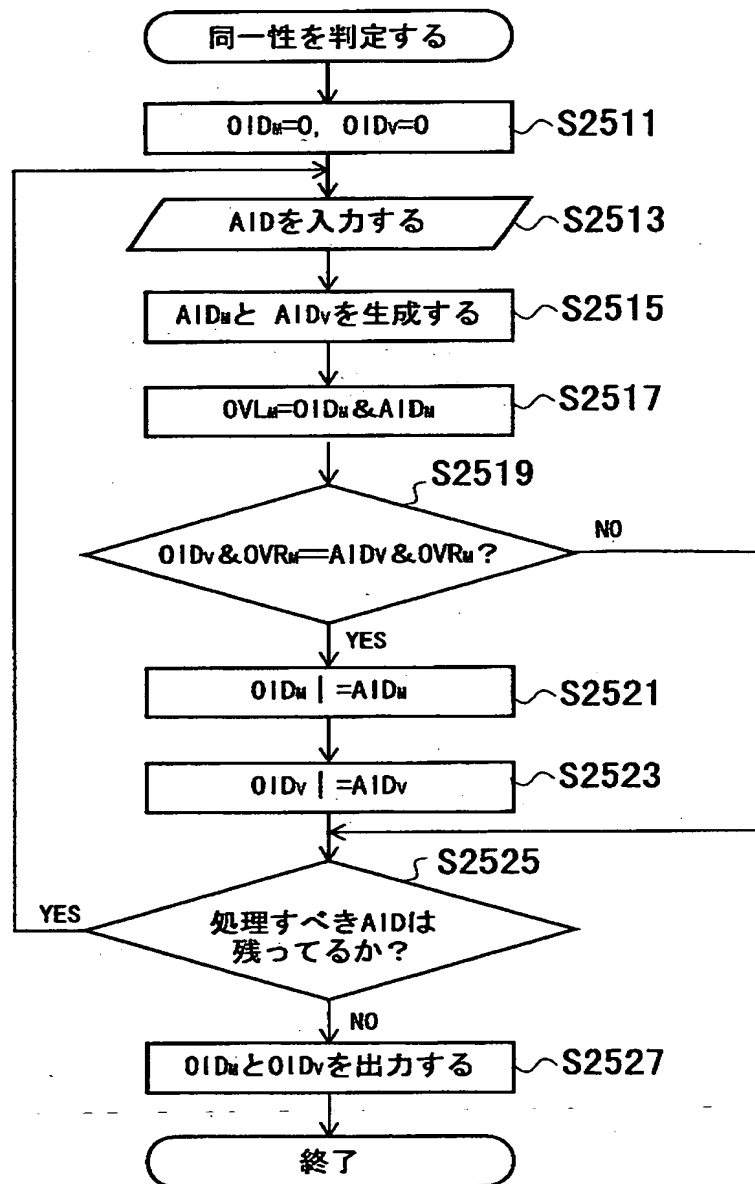
【図 2 4】

着信拒否申請・通知メッセージの例

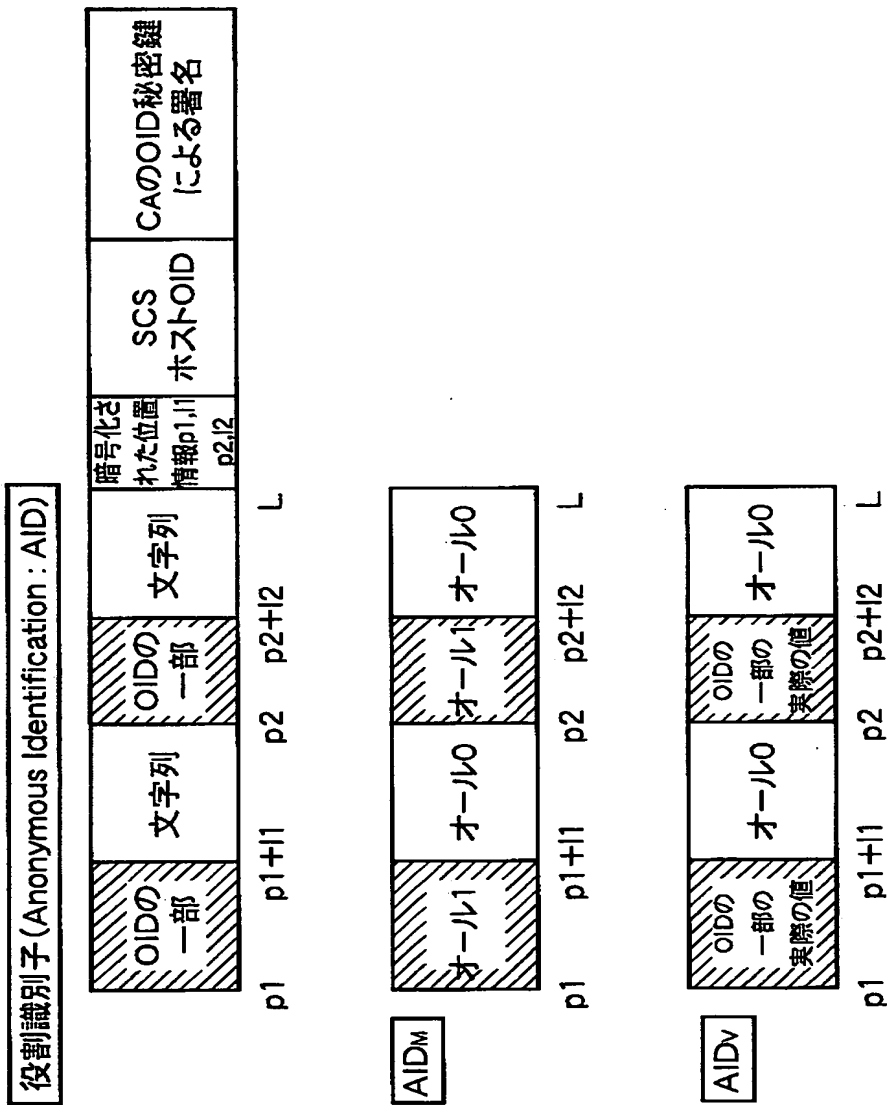
AIDの実体 REFUSE	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の設定の場合)
AIDの実体 RECONNECT	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の解除の場合)
<着信者AIDの秘密鍵による署名>	

AIDの実体 REFUSE	OKPAT, IPアドレス, ホスト名, ドメイン名の実体 (設定成功の場合)
AIDの実体 RECONNECT	NGPAT, IPアドレス, ホスト名, ドメイン名の実体 (解除失敗の場合, つまり, エラーメッセージ)
<着信者AIDの公開鍵による署名>	

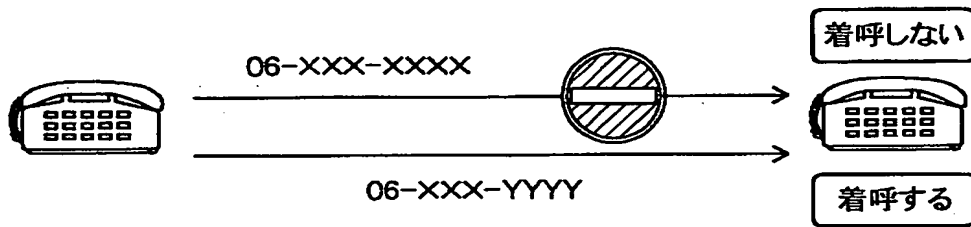
【図 25】



【図 26】

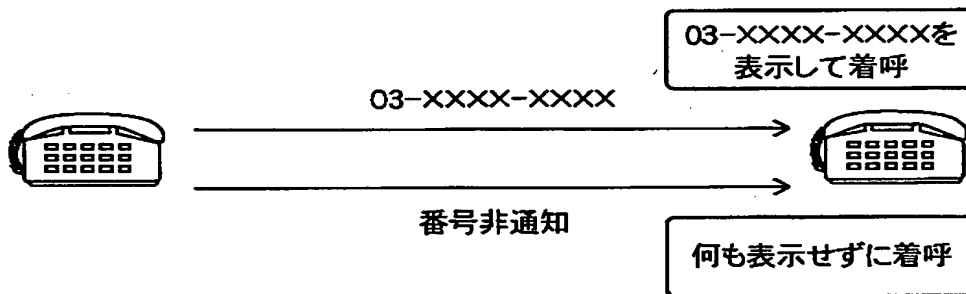


【図 27】



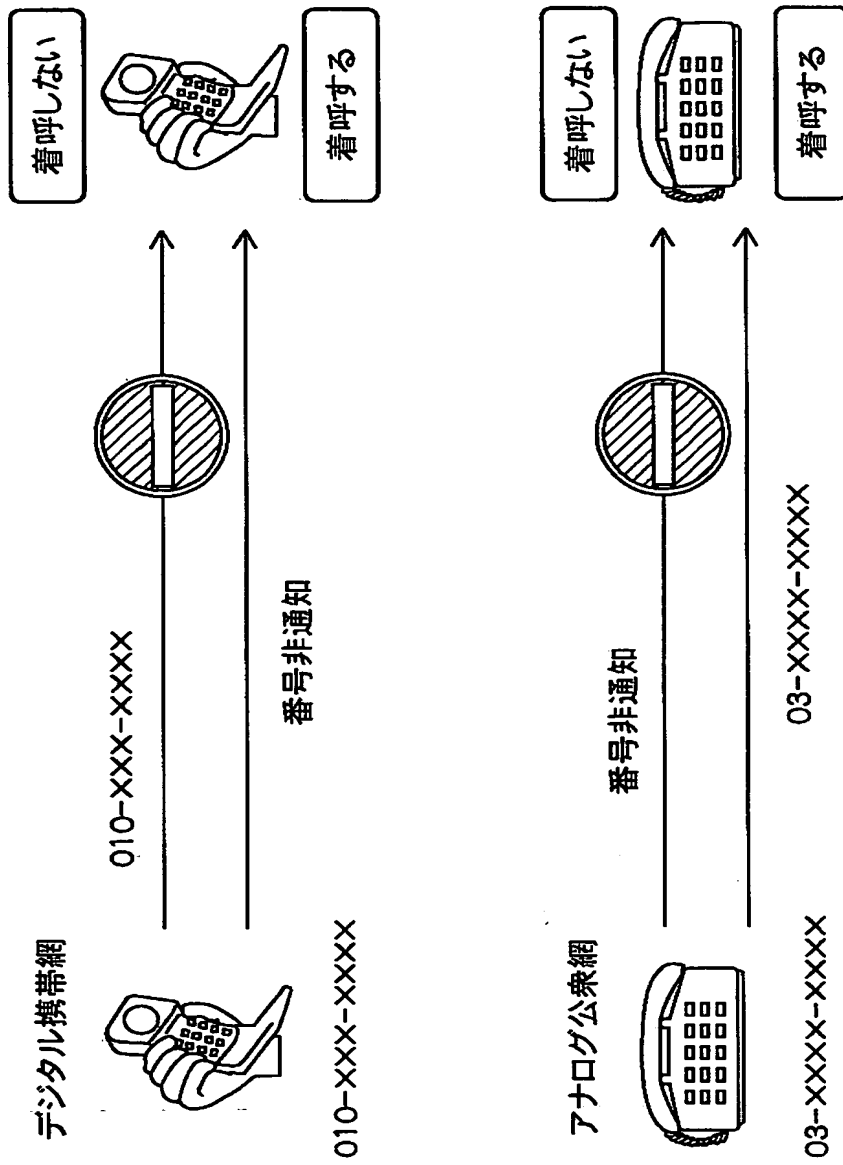
アナログ公衆網における二重番号登録

【図 28】



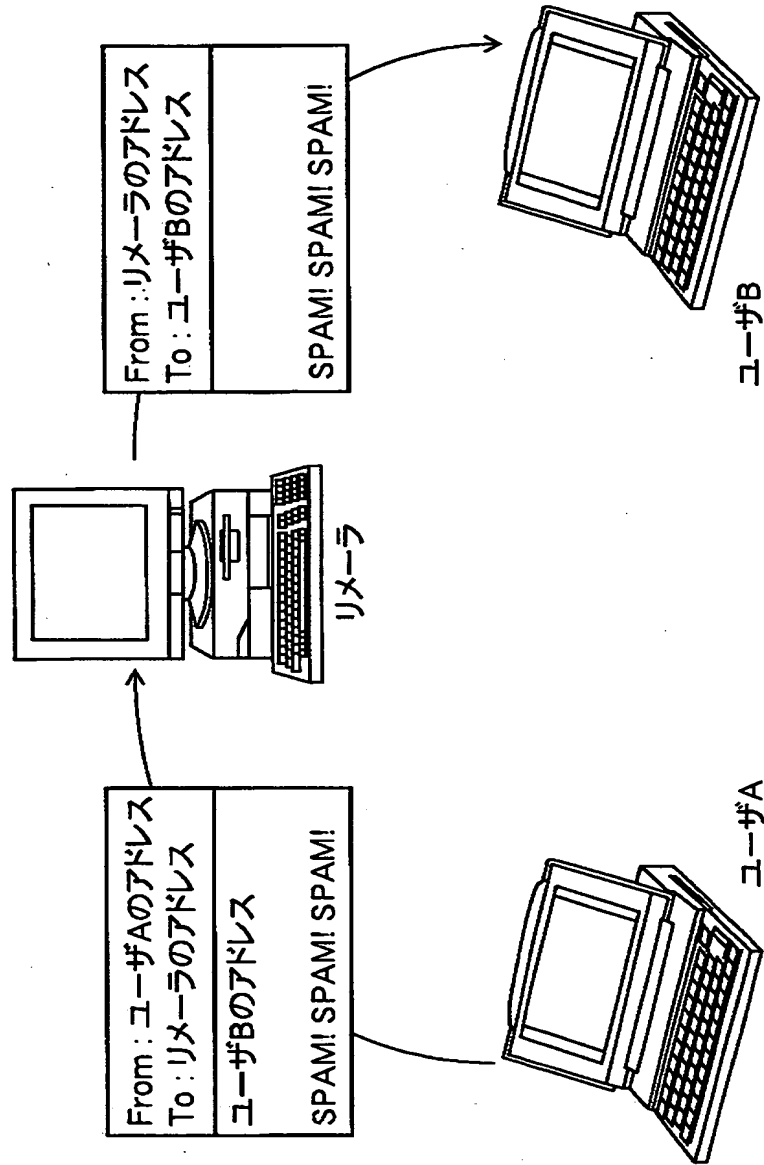
アナログ公衆網における発信者番号通知

【図 29】



デジタル携帯網・アナログ公衆網における着信拒否

【図 30】



匿名電子メール (Anonymous Mails)

【書類名】 要約書

【要約】

【課題】 匿名性とセキュリティを確保すべく着信者の匿名性を保持しつつ発信者からの通信の接続を可能とする接続制御方法および通信網を提供する。

【解決手段】 ユーザに役割識別子を付与し、役割識別子とユーザに関する情報を閲覧可能に保持し、発信者は着信者を役割識別子で指定し、この指定に基づき発信者に発信者フラグ、移転制御フラグ、有効期限を含む個別化アクセスチケットを発行し、役割識別子と個別化アクセスチケットを用いて個別化アクセスチケットが有効期限内で正当であり、発信者役割識別子が個別化アクセスチケットに含まれ、着信者役割識別子が個別化アクセスチケットに含まれていることを検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網に物理的な接続制御方式に変換する接続制御を行う。

【選択図】 図 1

【書類名】
【訂正書類】

職権訂正データ
特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000004226

【住所又は居所】 東京都新宿区西新宿三丁目19番2号

【氏名又は名称】 日本電信電話株式会社

【代理人】 申請人

【識別番号】 100083806

【住所又は居所】 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル
9階 三好内外国特許事務所

【氏名又は名称】 三好 秀和

【選任した代理人】

【識別番号】 100068342

【住所又は居所】 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル
9階 三好内外国特許事務所

【氏名又は名称】 三好 保男

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日

[変更理由] 住所変更

住 所 東京都新宿区西新宿三丁目19番2号

氏 名 日本電信電話株式会社